

**NORTH ATLANTIC TREATY ORGANISATION**



**RESEARCH AND TECHNOLOGY ORGANISATION**

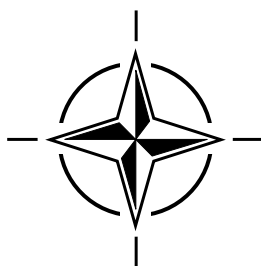
BP 25, 7 RUE ANCELLE, F-92201 NEUILLY-SUR-SEINE CEDEX, FRANCE

**RTO TECHNICAL REPORT 50**

# **NATO HLA Certification**

(Certification HLA OTAN)

*Work performed by the RTO NATO Modelling and Simulation Group Task Group 008.*



Published June 2002

*Distribution and Availability on Back Cover*

Report Documentation Page		
<b>Report Date</b> 01JUN2002	<b>Report Type</b> N/A	<b>Dates Covered (from... to)</b> -
<b>Title and Subtitle</b> NATO HLA Certification		<b>Contract Number</b>
		<b>Grant Number</b>
		<b>Program Element Number</b>
<b>Author(s)</b>		<b>Project Number</b>
		<b>Task Number</b>
		<b>Work Unit Number</b>
<b>Performing Organization Name(s) and Address(es)</b> Research and Technology Organisation North Atlantic Treaty Organisation BP 25, F-92201 Neuilly-sur-Seine Cedex, France		<b>Performing Organization Report Number</b>
<b>Sponsoring/Monitoring Agency Name(s) and Address(es)</b>		<b>Sponsor/Monitor's Acronym(s)</b>
		<b>Sponsor/Monitor's Report Number(s)</b>
<b>Distribution/Availability Statement</b> Approved for public release, distribution unlimited		
<b>Supplementary Notes</b> The original document contains color images.		
<b>Abstract</b>		
<b>Subject Terms</b>		
<b>Report Classification</b> unclassified		<b>Classification of this page</b> unclassified
<b>Classification of Abstract</b> unclassified		<b>Limitation of Abstract</b> SAR
<b>Number of Pages</b> 54		

**This page has been deliberately left blank**



**Page intentionnellement blanche**

**NORTH ATLANTIC TREATY ORGANISATION**



**RESEARCH AND TECHNOLOGY ORGANISATION**

BP 25, 7 RUE ANCELLE, F-92201 NEUILLY-SUR-SEINE CEDEX, FRANCE

---

**RTO TECHNICAL REPORT 50**

## **NATO HLA Certification**

(Certification HLA OTAN)

**By:**

Jean-Louis Igarza (TG chairman, RTA MSCO)

Pascal Cantot (France)

Mark Crooks (US)

Hans-Peter Menzler (Germany)

Andrzej Najgebauer (Poland)

Neil Smith (UK)

Philomena Zimmerman (US)

*Work performed by the RTO NATO Modelling and Simulation Group Task Group 008.*



# The Research and Technology Organisation (RTO) of NATO

RTO is the single focus in NATO for Defence Research and Technology activities. Its mission is to conduct and promote cooperative research and information exchange. The objective is to support the development and effective use of national defence research and technology and to meet the military needs of the Alliance, to maintain a technological lead, and to provide advice to NATO and national decision makers. The RTO performs its mission with the support of an extensive network of national experts. It also ensures effective coordination with other NATO bodies involved in R&T activities.

RTO reports both to the Military Committee of NATO and to the Conference of National Armament Directors. It comprises a Research and Technology Board (RTB) as the highest level of national representation and the Research and Technology Agency (RTA), a dedicated staff with its headquarters in Neuilly, near Paris, France. In order to facilitate contacts with the military users and other NATO activities, a small part of the RTA staff is located in NATO Headquarters in Brussels. The Brussels staff also coordinates RTO's cooperation with nations in Middle and Eastern Europe, to which RTO attaches particular importance especially as working together in the field of research is one of the more promising areas of initial cooperation.

The total spectrum of R&T activities is covered by the following 7 bodies:

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS Studies, Analysis and Simulation Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These bodies are made up of national representatives as well as generally recognised 'world class' scientists. They also provide a communication link to military users and other NATO bodies. RTO's scientific and technological work is carried out by Technical Teams, created for specific activities and with a specific duration. Such Technical Teams can organise workshops, symposia, field trials, lecture series and training courses. An important function of these Technical Teams is to ensure the continuity of the expert networks.

RTO builds upon earlier cooperation in defence research and technology as set-up under the Advisory Group for Aerospace Research and Development (AGARD) and the Defence Research Group (DRG). AGARD and the DRG share common roots in that they were both established at the initiative of Dr Theodore von Kármán, a leading aerospace scientist, who early on recognised the importance of scientific support for the Allied Armed Forces. RTO is capitalising on these common roots in order to provide the Alliance and the NATO nations with a strong scientific and technological basis that will guarantee a solid base for the future.

The content of this publication has been reproduced directly from material supplied by RTO or the authors.

Published June 2002

Copyright © RTO/NATO 2002  
All Rights Reserved

ISBN 92-837-1087-8



*Printed by St. Joseph Print Group Inc.  
(A St. Joseph Corporation Company)  
1165 Kenaston Street, Ottawa, Ontario, Canada K1G 6S1*

# **NATO HLA Certification**

**(RTO TR-050 / NMSG-011)**

## **Executive Summary**

In 1998, the North Atlantic Council (NAC) approved the creation of a new organisation tasked with co-ordinating the modelling and simulation (M&S) activities of the Alliance. This Organisation, known as the NATO Modelling and Simulation Group (NMSG), was set up inside the Research and Technology Organisation (RTO). The activities of NMSG are set out in an M&S action plan (MSAP) approved by the RTO Board. This document stresses that the HLA interoperability standard was chosen in 1998 as the basic standard on which the future common technical framework (CTF) of the Alliance for M&S activities will be established.

The need to certify the compliance of simulations with the standard was established right from the initial development stage of the HLA. At present, this capability exists only in the United States, but this country is temporarily offering its support to NATO and its allies free of charge. As part of its action plan, NMSG decided to form a working group tasked with comparing various possibilities of setting up an HLA compliance certification capability for simulations developed and used by NATO.

This working group (MSG-011) met 4 times in 2001 (in May, in July, in September and in December) and produced this report. It was chaired by the NATO M&S Co-ordination Office (MSCO) and the following nations took part in it:

- France,
- Germany,
- Poland,
- United Kingdom,
- United States.

The first chapter of the report briefly describes the HLA interoperability standard and the history of its adoption by NATO. It tries to show why it is useful and important to implement a compliance certification capability for the standard within the Alliance. The second chapter describes the certification process already in force in the US, as well as the conditions and resources required for its implementation. Chapter 3 gives the positions of the member nations of MSG 011 concerning HLA certification. Chapter 4 deals with the different conditions and constraints to be taken into account when envisaging an HLA certification capability within NATO. Chapter 5 describes and assesses three possible solutions:

- The creation of a NATO certification centre,
- The hire of the US capability by NATO,
- The setting up of a capability to be distributed among volunteer nations.

Chapter 6 provides recommendations for the establishment of this capability. The recommended solution is the third one: The setting up of an HLA certification capability to be distributed among volunteer nations. There are a number of advantages to this solution: it is simple for NATO to implement from the administrative and financial points of view. It also offers nations who express national requirements the possibility of satisfying them. The most urgent stages to be completed in order to enable implementation of this solution are, first, the decision on the part of the nations to declare themselves volunteers, and second, the creation of a users club responsible for supervising implementation of the certification process and its future developments, in line with changes in the HLA standard and the constraints imposed on the Alliance and its member countries.

# Certification HLA OTAN

(RTO TR-050 / NMSG-011)

## Synthèse

En 1998, le Conseil de l'Atlantique Nord (NAC) approuvait la création d'une nouvelle organisation chargée de coordonner les activités de l'Alliance en matière de Modèles et Simulations (M&S). Cette organisation, appelée groupe OTAN pour les M&S (NMSG), a été implantée au sein de l'organisation de recherche et technologie (RTO). Les activités du NMSG sont organisées selon un plan d'action M&S (MSAP) approuvé par le comité directeur de la RTO. Ce document rappelle, en particulier, que le standard d'interopérabilité HLA (High Level Architecture) a été choisi en 1998 comme le standard de base sur lequel sera établi la future infrastructure technique commune (CTF) de l'Alliance pour les M&S.

Dès le développement initial de la HLA, le besoin de certifier la conformité des simulations au standard a été identifié. Actuellement, cette capacité existe uniquement aux Etats-Unis qui offre provisoirement et gratuitement son soutien à l'OTAN et à ses alliés. Dans le cadre de son plan d'action, le NMSG a décidé la création d'un groupe de travail chargé de comparer différentes possibilités pour implanter une capacité de certification de conformité au standard HLA des simulations développées et utilisées par l'OTAN.

Ce groupe de travail (le MSG-011) s'est réuni à quatre reprises en 2001 (Mai, Juillet, Septembre et Décembre) et a rédigé ce rapport. Il était présidé par le bureau OTAN de coordination des M&S (le MSCO) et les nations suivantes y ont participé :

- Allemagne,
- Etats-Unis,
- France,
- Pologne,
- Royaume-Uni.

Le premier chapitre du rapport décrit brièvement le standard d'interopérabilité HLA et rappelle l'historique de son adoption par l'OTAN. Il s'efforce d'expliquer pourquoi il est utile et important d'implémenter une capacité de certification de conformité au standard dans l'Alliance. Le second chapitre décrit le processus de certification déjà en service aux Etats-Unis ainsi que les conditions et les moyens utilisés pour sa mise en œuvre. Au chapitre 3, sont exposées les positions des pays membres du MSG 011 sur la certification HLA. Le chapitre 4 traite des conditions et contraintes diverses à prendre en compte en vue d'établir une capacité de certification HLA à l'OTAN. Le chapitre 5 décrit et évalue trois solutions possibles :

- Etablissement d'un centre OTAN de certification,
- Location de la capacité des Etats-Unis par l'OTAN,
- Implantation d'une capacité distribuée parmi des nations volontaires.

Le chapitre 6 donne des recommandations pour la création de cette capacité. La solution recommandée est la troisième : la mise en place d'une capacité de certification HLA distribuée parmi des nations volontaires. Les avantages de cette solution sont nombreux : sa mise en œuvre est simple pour l'OTAN sur les plans administratif et financier. Elle offre en outre aux nations qui exprimeront des besoins nationaux la possibilité de les satisfaire. Les étapes les plus urgentes à franchir pour mettre en œuvre cette solution sont, d'abord, la décision des nations de se porter volontaires, ensuite la création d'un club d'utilisateurs chargé de superviser la mise en œuvre du processus de certification et ses évolutions futures, en cohérence avec les évolutions du standard HLA et les contraintes de l'Alliance et des pays membres.

# Contents

	<b>Page</b>
<b>Executive Summary</b>	<b>iii</b>
<b>Synthèse</b>	<b>iv</b>
<b>NMSG-011-TG-008 Members, Authors and Contributors</b>	<b>vii</b>
<b>1. Introduction</b>	<b>1</b>
<b>1.1 HLA Description</b>	<b>1</b>
1.1.1 Generality	1
1.1.2 Functional Overview	2
1.1.3 Formal Definition of the HLA Standard	3
1.1.3.1 HLA Interface Specification	3
1.1.3.2 HLA Object Models	3
1.1.3.3 HLA Rules	4
<b>1.2 Adoption of HLA as the NATO Interoperability Standard</b>	<b>4</b>
<b>1.3 Technical Activity Description</b>	<b>5</b>
<b>1.4 HLA Certification Rationale</b>	<b>5</b>
<b>2. The Current US Certification Process</b>	<b>7</b>
<b>2.1 The Process</b>	<b>7</b>
<b>2.2 Required Resources</b>	<b>8</b>
2.2.1 Human Resource Requirements	8
2.2.2 Software Requirements	8
2.2.3 Hardware Requirements	9
<b>3. National Requests and Positions on HLA Certification</b>	<b>11</b>
<b>3.1 France</b>	<b>11</b>
<b>3.2 Germany</b>	<b>11</b>
<b>3.3 Poland</b>	<b>12</b>
<b>3.4 UK</b>	<b>13</b>
<b>3.5 US</b>	<b>13</b>
<b>3.6 Summary of National Positions</b>	<b>14</b>
<b>4. Conditions and Constraints for Establishing a NATO Capability</b>	<b>15</b>
<b>4.1 Resourcing / Funding Issues</b>	<b>15</b>
<b>4.2 Relationship with other Organisations</b>	<b>15</b>
4.2.1 US Help Desk	15
4.2.2 Re-Use Paradigm	16
<b>4.3 Reference HLA STANAG</b>	<b>16</b>
<b>4.4 M&amp;S Community Awareness</b>	<b>16</b>
<b>4.5 Partnership for Peace Issues</b>	<b>17</b>
<b>4.6 Test Suite Enhancement Issues</b>	<b>18</b>
4.6.1 Software	18
4.6.2 Increased Testing Scope	18
4.6.2.1 General Issues for Discussion	19
4.6.2.2 Middleware Issues	19
4.6.2.3 Provisional Conclusion	20
<b>4.7 Security and Proprietary Information Issues</b>	<b>21</b>



<b>5. Different Implementation Hypotheses</b>	<b>23</b>
<b>5.1 Permanent NATO Certification Centre</b>	<b>23</b>
5.1.1 Location	23
5.1.2 Funding	23
5.1.3 Working Conditions	24
5.1.4 Use of the NATO Facility to Meet National Requirements	24
5.1.5 Provisional Conclusion on the Establishment of a Permanent NATO Capability	24
<b>5.2 Rental of National US Certification Capability by NATO</b>	<b>25</b>
5.2.1 US Policy on Future Capability	25
5.2.2 Description of Capability and Assessment of Costs, Prioritisation of Requests	25
5.2.3 “Do Nothing” Option	25
5.2.4 Perception Issues	26
<b>5.3 Establishing a NATO Capability Voluntary Supported by NATO Nations</b>	<b>26</b>
5.3.1 Description	26
5.3.2 General Conditions	27
5.3.3 Provisional Conclusion	27
<b>5.4 Solutions’ Assessment</b>	<b>27</b>
<b>6. Conclusions and Recommendations</b>	<b>29</b>
<b>6.1 Justification for NATO HLA Certification</b>	<b>29</b>
<b>6.2 Preferred Solution</b>	<b>29</b>
<b>6.3 Evolution of the HLA Certification Process</b>	<b>30</b>
<b>6.4 Next Step Proposals</b>	<b>30</b>
<b>Annex A – US Technical Area Task (TAT) Process</b>	<b>31</b>
<b>Annex B – US Subscription Account Process</b>	<b>33</b>
<b>Annex C – List of Acronyms</b>	<b>35</b>
<b>Annex D – References</b>	<b>39</b>

# **NMSG-011-TG-008**

## **Members, Authors and Contributors**

### **GROUP OFFICERS**

#### **NMSG Chairman:**

Dir BWB E. SCHWAN  
BWB FE 1  
Postfach 7360  
Konrad-Adenauer-Ufer 2-6  
D-56057 Koblenz  
GERMANY

#### **NMSG Vice-Chairman:**

Ms L.E. McGLYNN  
Special Asst to ODUSA (OR) for M&S  
and Light Forces Studies  
Room 1E643, Pentagon  
Washington, DC 20310  
U.S.A.

### **TASK GROUP 008 MEMBERS**

#### **Chairman**

##### **Mr Jean-Louis IGARZA**

Chief Scientist  
RTA/NMSCO  
BP 25, F-92201 Neuilly-sur-Seine Cedex  
FRANCE  
Tel : +33 (0) 1 55 61 22 77  
Fax : +33 (0) 1 55 61 22 99  
e-mail : igarzaj@rta.nato.int

#### **Members**

##### **IETA P. CANTOT**

DGA/DSP/STTC  
26, Boulevard Victor  
00460 ARMEES  
FRANCE  
Tel : +33 (0)1 45 52 46 88  
Fax : +33 (0)1 45 52 46 92  
e-mail : cantotp@wanadoo.fr

##### **Mr Hans-Peter MENZLER**

WTD 81/Simulationsinfrastruktur  
Kalvarienberg  
D-91171 Greding  
GERMANY  
Tel : +49 84 63 652 599  
Fax : +49 84 63 652 607  
e-mail : hpmenzler@bwb.org

##### **Col. Andrzej NAJGEBAUER**

Deputy Dean of Faculty of Cybernetics  
Military University of Technology  
2, Kaliskiego Str.  
00-908 Warsaw 49  
POLAND  
Tel : +48 22 683 94 29  
Fax : +48 22 683 72 62  
e-mail : anajgeb@isi.wat.waw.pl

##### **Mr Neil SMITH**

Simulation & Synthetic Environment (SEs)  
Platform Systems & Technology  
DSLTI/Integrated Systems  
Room 126, Bldg 115  
Bedford Technology Park  
Bedford, MK41 6AE  
UNITED KINGDOM  
Tel : +44 1234 71 64 36  
Fax : +44 1234 71 64 40  
e-mail : nsmith@dstl.gov.uk

##### **Ms Philomena ZIMMERMAN**

HLA Program Manager  
Defense Modeling & Simulation Office  
1901 N. Beauregard St.  
Suite 500  
Alexandria, VA 22311  
UNITED STATES  
Tel : +1 703 998 0660  
Fax : +1 703 998 0667  
e-mail : pzimmerm@dmsomil

**Authors/Contributors**

**Mr Jean-Louis IGARZA**  
**IETA P. CANTOT**  
**Mr Hans-Peter MENZLER**  
**Col. Andrzej NAJGEBAUER**  
**Mr Neil SMITH**  
**Ms Philomena ZIMMERMAN**

**Mr Mark CROOKS**  
Defence Modeling & Simulation Office  
1901 N. Beauregard St.  
Suite 400  
Alexandria, VA 22311  
UNITED STATES  
Tel : +1 703 933 3312  
Fax : +1 703 933 3325  
e-mail : mcrooks@msiac.dmsomil

**NATO Modelling and Simulation Co-Ordination Office  
(RTA/NMSCO)**

**Mr. G.J. Burrows** (Head)  
**Cdr.G. Ameyugo Catalan** (Deputy, Head)  
**Mr Jean-Louis Igarza** (Chief Scientist)  
Research and Technology Agency  
BP 25, F-92201 Neuilly-sur-Seine Cedex  
FRANCE  
msg@rta.nato.int

# Chapter 1

## 1. Introduction

### 1.1. HLA Description

*This short description of HLA is derived from a US paper, written in Fall 1998 and presented in France, by Dr. Judith Dahmann. She was at that time the Chief Scientist of the United States Department of Defense (US DoD) Defense M&S Office (DMSO). The original text has been slightly modified to fit to the purpose of the present report and to reflect new features or events that occurred since the time it was published.*

#### 1.1.1 Generality

The High Level Architecture was developed by the US DoD in response to the clear recognition of the value of simulation to support a wide variety of military applications, as well as the need to manage simulations to ensure they provide a cost effective tool. In particular, simulations developed for one purpose can be readily reused in other applications, either individually or in combination. This reuse and interoperability is critical if simulations are to be affordable and useful to the changing needs of the DoD.

In response, the High Level Architecture (HLA) was developed, a preliminary version was published in 1995, and then HLA was mandated for use across DoD, in 1996.

***The HLA is a technical architecture developed to facilitate the reuse and interoperation of simulations.***

The HLA is based on the premise that no simulation can satisfy all uses and users. An individual simulation or set of simulations developed for one purpose can be applied to another application under the HLA concept of the ***federation***: a composable set of interacting simulations. The intent of the HLA is to provide a structure which will support reuse of capabilities available in different simulations, ultimately reducing the cost and time required to create a synthetic environment for a new purpose and providing developers the option of distributed collaborative development of complex simulation applications.

The HLA has wide applicability, across a full range of simulation application areas, including education and training, analysis, engineering and even entertainment, at a variety of levels of resolution. These widely differing application areas indicate the variety of requirements that have been considered in the development and evolution of the HLA.

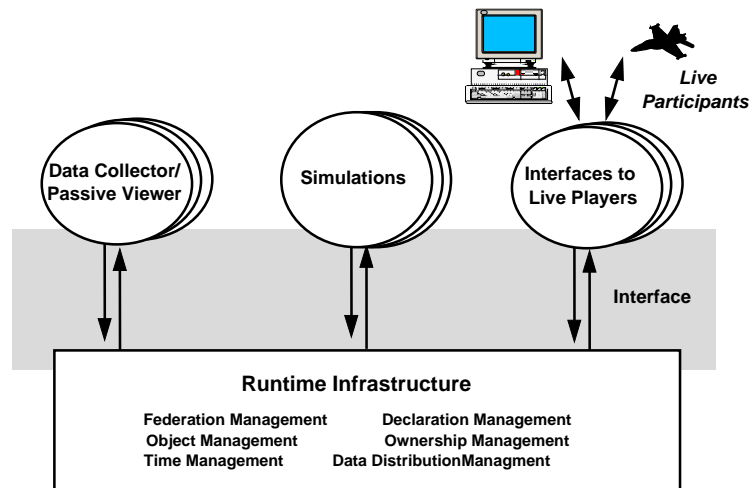
The selected definition of an architecture as intended in HLA -- "major functional elements, interfaces, and design rules, pertaining as feasible to all simulation applications, and providing a common framework within which specific system architectures can be defined" -- is one that is commonly accepted and is consistent with the definition of architecture for computer simulations provided by the Institute of Electronic Electricity Engineering (IEEE). For the purpose of this effort, the emphasis is on the development of a high level architecture which pertains as widely as possible to all simulation areas and which will provide a framework for the development of specific system architectures.

The HLA does not prescribe a specific implementation, nor does it mandate the use of any particular set of software or programming language. Over time, as technology advances become available, new and different implementations will be possible within the framework of the HLA. The technical specifications for the HLA are currently 1.3 which is available from the US DoD (see reference [3] to [5]), and 1516 which has been available from IEEE as an Open Standard since September 2000 (see reference [6] to [8]). Software to support HLA is now available or in development by both government organisations and industry.

### 1.1.2. Functional Overview

Figure 1 shows how an HLA federation partitions into its major functional components.

The **first key component** is the set of simulations, or more generally, the *federates*. Examples of federates can include an event driven simulation, a real-time human-in-the-loop simulator, live equipment or a supporting utility (such as a viewer or data collector), or even an interface to a live player or instrumented facility. All object representation is in the federates. The HLA imposes no constraints on what is represented in the federates or how it is represented, but it does require that all federates incorporate specified capabilities to allow the objects in the simulation to interact with objects in other simulations. This is achieved through the exchange of data supported by services implemented in a common federate communications interface, referred to as a “Runtime Infrastructure” (RTI).



**Figure 1. Functional view of an HLA federation**

The **second functional component** is the *Runtime Infrastructure (RTI)*. As stated above the RTI is, in effect, a common communications interface for the federation. The RTI provides a very general purpose set of services that support the simulations in carrying out these federate-to-federate interactions and federation management support functions. These services will be discussed in a subsequent section. All interactions among the federates go through the RTI.

The **third functional component** is the *runtime interface*. The HLA runtime interface specification provides a standard way for federates to interact with the RTI, to invoke the RTI services to support runtime interactions among federates and to respond to requests from the RTI. *This interface is implementation independent* and is independent of the specific object models and data exchange requirements of any federation.

Two other general capabilities of simulation systems are supported by the architecture. First, the HLA supports the passive collection of simulation data and monitoring of simulation activities. In the HLA, these tools act in the same way as simulations and interact with the RTI using the HLA interface.

Second, the HLA supports interfaces to live participants, such as instrumented platforms (such as real aircraft) or live systems (such as C4I systems). Live participants interact with the simulated world through something that acts like a simulation from the point of view of the HLA, that feeds a representation of the live world into the simulated world and that projects data from the simulated world back to the live system.

The HLA standard is formally defined by three components, i.e.

- the interface specification,
- the object model template,
- and the HLA rules.

### 1.1.3. Formal Definition of the HLA standard

According to Warren KATZ, chairman of the Simulation Interoperability Standards Organisation (SISO), a standard in the M&S domain is a “*written technical specification that enables unrelated parties to implement a technical solution that enables a level of interoperability between the independently developed solutions*”. While this statement provides a very general definition of the HLA, the NMSG-011 Task Group emphasises that standards must have been approved by a recognised ‘standards’ body, e.g. IEEE.

More specifically, the HLA standard is defined by the above-mentioned three components:

#### 1.1.3.1. HLA INTERFACE SPECIFICATION

The *HLA interface specification* describes the runtime services provided to the federates by the RTI, and by the federates to the RTI. There are seven classes of services.

- *Federation management* services offer basic functions required to create and operate a federation.
- *Declaration management* services support efficient management of data exchange through the information provided by federates defining the data they will provide and will require during a federation execution.
- *Object management* services provide creation, deletion, identification and other services at the object level.
- *Ownership management* services support the dynamic transfer of ownership of object/attributes during an execution.
- *Time management* services support synchronisation of runtime simulation data exchange.
- *Data distribution management* services support the efficient routing of data among federates during the course of a federation execution.
- Some other miscellaneous services are also provided or used that are difficult to classify in the six previous categories.

The HLA interface specification defines the way these services are accessed, both functionally and in an application programmer's interface (API). APIs that are currently available include those implemented in CORBA IDL (see Annexe D), C++, Ada, and Java.

#### 1.1.3.2. HLA OBJECT MODELS

*HLA object models* are descriptions of the essential sharable elements of the simulation or federation in 'object' terms. The HLA is directed towards interoperability; hence in the HLA, object models are intended to focus on description of the critical aspects of simulations and federations, which are shared across a federation. The HLA puts no constraints on the content of the object models. The HLA does require that each federate and federation document its object model using a standard object model template. These templates are intended to be the means for open information sharing across the community to facilitate reuse of simulations. These completed templates are often openly available, and tools are available or being developed to allow for automated search and reasoning about object model template data, to further facilitate cost-effective information exchange and reuse.

The HLA specifies two types of object models: the HLA Federation Object Model (FOM) and the HLA Simulation Object Model (SOM). The HLA FOM describes the set of objects, attributes and interactions, which are shared across a federation. The HLA SOM describes the simulation (federate) in terms of the types of objects, attributes and interactions it can offer to future federations. The SOM is distinct from internal design information; rather it provides information on the capabilities of a simulation to exchange information as part of a federation. The SOM is essentially a contract by the simulation defining the types

of information it can make available in future federations. The availability of the SOM facilitates the assessment of the appropriateness of the federate for participation in a federation.

While the HLA does not define the contents of a SOM or FOM, it does require that a common documentation approach be used. Both the HLA FOM and SOM are documented using a standard form called the HLA Object Model Template (OMT).

### 1.1.3.3. HLA RULES

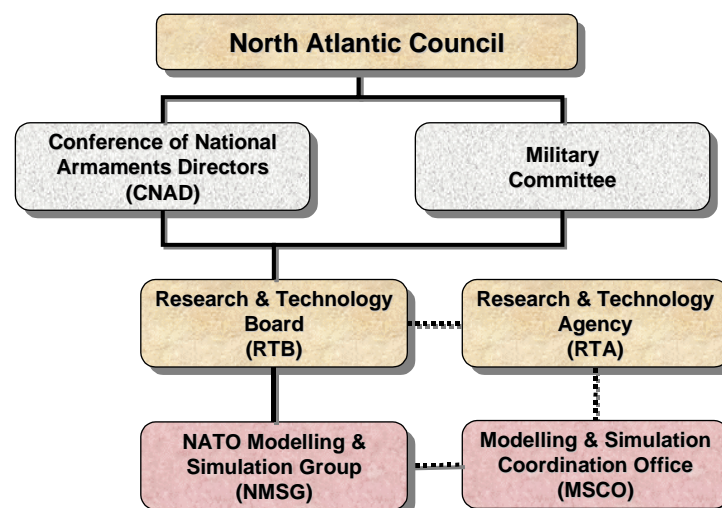
Finally, the **HLA rules** summarise the key principles behind the HLA. The rules are divided into two groups: federation and federate rules. Federations, or sets of interacting simulations or federates, are required to have a FOM in the OMT format. During runtime, all object representation takes place in the federates (not in the RTI) with only one federate owning any given attribute of an instance of an object at any given time. Information exchange among the federates takes place via the RTI using the HLA interface specification.

Additional rules apply to individual federates. Under the HLA, each federate must document their public information in their SOM using the OMT. Based on the information included in their SOM, federates must import and export information, transfer object attribute ownership, updates attributes and interact with the time management services of the RTI when managing local time.

## 1.2. Adoption of HLA as the NATO interoperability standard

In 1996 a temporary working group was set-up within NATO to assess the possibility of establishing a permanent M&S organisation within the Alliance. This working group was named the Steering Group for M&S (SGMS) and reported to both the Conference of National Armaments Directors (CNAD) and the Military Committee (MC), via the Research and Technology Organisation (RTO).

In 1998, the SGMS published two documents: a final report proposing a NATO M&S organisation and a NATO M&S Master Plan (MSMP). Both documents were approved by first the above-mentioned hierarchy (RTO, CNAD and MC) and finally by the North Atlantic Council in November 1998. Since then the M&S organisation has been set up under the auspices of the RTO, as shown on the following drawing.



Concerning the standardisation aspect, both the approved MSMP and the SGMS final report have recognised the HLA as the NATO main M&S interoperability standard. Since then HLA is being progressed to become an official NATO standard (a STANAG).

### 1.3. Technical Activity Description

The origin of this RTA technical activity comes directly from the objective 1 of the NATO M&S Master Plan (Establish a common M&S architecture) and, more specifically, from sub-objective 1.1 which recommends the adoption of HLA as the interoperability standard for NATO. The US experience on the HLA has demonstrated the interest of establishing an HLA compliance certification capability. The interest of this approach is explained in detail in the paragraph 1.4. The establishment of an HLA compliance certification capability is not precisely identified within the Master Plan as an objective, but its existence is mentioned as an evidence. At the beginning of the NMSG activity (1999), the US proposed to support NATO with this capability, waiting for NATO or some other member nations to establish their own capability. In response to this, the NMSG started to investigate how to implement a similar capability within NATO. Subsequently this NMSG technical activity was approved by the RTB in Spring 2000 and actually started work in May 2001, when participating nations were identified.

Nations supporting this activity are France, Germany, Poland, UK and US. The task group is chaired by the MSCO. The work was completed in an eighth-month timeframe. The main deliverable of this work is this report and the recommendations that it is providing. The main objective assigned to the task group in its TOR was to “Do a investment/appraisal benefit analysis for establishing a NATO capability in assuming that the US capability becomes unavailable”. There was no need to assess the likelihood of the above mentioned hypothesis since it appears that the US does not plan to stop its certification activity in the short term and has even agreed to continue, providing its support to NATO. However, it is hoped that the general objective has been globally addressed.

The current US HLA certification activity concerns two different but interrelated activities, i.e.

- First, the HLA compliance certification of federates which has a direct interest for NATO with respect to enhancing its capability for establishing and running HLA federations for its own operational requirements,
- Second, the verification that commercial or government-supported RTIs comply with the HLA standard.

The activity associated with verifying HLA RTIs has been recognised by the task group as very important for the overall M&S community, but this is a very technical and specific issue which could not be addressed by NATO as a priority area. Consequently there was no requirement identified in the Master Plan for establishing such a capability within NATO or member nations. This issue has therefore not been addressed in the present work.

### 1.4. HLA Certification Rationale

When compiling a distributed simulation, all aspects of interoperability must be examined, in order to add some stability to the process of federating. Some interoperability aspects may need a federation level investigation, while others can be accomplished by the individual federates, and declared, or stated during federation gatherings. The federation manager (or designated individual) can perform the interoperability assurance a variety of ways; and it may be prudent for the federation manager to employ many methods. One of the best, unbiased methods is to examine federate “certification”.

Concerns and problems associated with interoperability are currently categorised into two broad areas: technical interoperability, and substantive interoperability. Technical interoperability is the capability of federates to physically connect and exchange data in accordance with the HLA standard. Substantive interoperability is driven by the needs of the federation and has to be addressed by each federation in a federation specific way. HLA federate compliance deals only with technical interoperability. However this is a prerequisite for substantive interoperability assurance.

In the HLA, there is currently an accepted set of tests under which a federate can receive a level of compliance, based on their stated inputs to a variety of steps (see Section 2), and their ability to meet the standards. The tests are conducted by an independent organisation, and employ a standard set of tools and



question and answer sessions. These do not totally satisfy all the interoperability concerns of a federation manager, but do provide a level of assurance that:

- the federate produces and consumes what it claims it can,
- the federate manages itself in a manner consistent with what it claims,
- the federate can call and receive call-backs from a verified RTI as it states it can.

The need to check HLA compliance has resulted in a US HLA compliance testing process specifically aimed to evaluate simulations and certify them as HLA compliant to HLA Rules, Interface Specification and the Object Model Template (OMT). The requirements for a compliance testing method and a set of relevant support tools were identified in early HLA development projects, including the “HLA proto-federations” which were developed in 1996.

Awareness and availability of the HLA compliance testing process is to be considered a technical help to facilitate the integration of federates in a federation, saving time and money, in addition to encouraging reuse of federate applications. Experiences of some past federations within NATO/Europe where the compliance testing process was not used include the NATO DiMuNDS experiment (2000) and the UK Future Offensive Air System (FOAS) Synthetic Environment (2000). As a consequence of not using this process the developers on each of these projects were forced to re-invent a local Federate Testing Process (FTP) to test the capability for each federate to interface to the HLA federation in accordance with the HLA standard.

The experience of other distributed simulation standards such as DIS have demonstrated that technical people have the tendency to deviate from the documented standard. In the case of DIS this was because the set of defined protocols were considered to be too rigid and subsequently could not cover all their requirements. Although the HLA philosophy is more flexible than the DIS Standard, HLA interoperability requires a strict adherence to the current version of the standard. The consequence of some former practices as outlined earlier in DIS was a loss of reuse capability and also a lack of interoperability when using DIS support tools or when adding new simulations to extend the capability of a pre-existing federation.

One of the two objectives of the NATO MSMP is the reuse of simulations. In this context the HLA testing process forces the development of SOMs in the HLA paradigm and provides the best way to record SOMs in a repository, which subsequently facilitates the reuse of federates. Typically, SOMs are not a prerequisite for interoperating federates when considering only the software aspect - only a FOM and a RTI are really required from the technical point of view to interconnect federates. However, the availability of SOMs provides some guarantee on the claimed capability of the federates, even if it is not a full insurance of their interoperability.

The compliance tests provide a first level of assurance to the federation manager that the federate conducts itself as it says it can. However, this is not the answer to the entire interoperability issue of the federation manager. For example the functional capabilities of a given federate are likely to evolve once initial compliance certification has been achieved. However, the fact remains that following this first step the federate knows how the HLA operates, and what is expected of both the HLA, and itself. Indeed, because of the documentation required during the compliance process, when capabilities of the federate changes, it is merely matter of updating documentation, which is already in the correct format. It is recommended that federates should be re-certified when significant changes have been introduced, such as the use of additional HLA services, changes to the SOM or implementation of a different interface specification.

It is very important to have a formal method to verify that developers of modelling and simulation applications (e.g. HLA federate developers), understand the HLA concept and associated standard. In this context the HLA compliance testing process should be considered as an integral part of the High Level Architecture.

## Chapter 2

### 2. The current US certification process

Compliance with the High Level Architecture (HLA) was mandated for U.S. Department of Defense (DoD) simulations in 1996 [1] and reaffirmed in 1998 [2]. The Defense Modeling and Simulation Office (DMSO) established a federate compliance test process to evaluate simulations and certify them as HLA compliant to HLA Rules, Interface Specification and the Object Model Template (OMT). Testing began in October 1997 and as of November 2001 over 220 federates have undergone HLA compliance testing.

The process is described below. Additional information is available via the DMSO Web Site and questions may be submitted to [hla@dmsomil](mailto:hla@dmsomil) or in reference [9].

#### 2.1 The Process

The overall process is quite simple. To be certified as HLA compliant, a federate must demonstrate its adherence to the three specification documents defining the HLA: the HLA Rules, the Interface Specification, and the Object Model Template Specification (references [3] to [5]). The current process has four steps outlined here.

**Step 1:** Complete a test application via test web page. Information needed to complete the application includes:

- Point of Contact Information
- Sponsorship Information
- Federate Name, Version, and Brief Description
- HLA Specification Version
- RTI Version (verified using DMSO RTI verification process)
- Expected Interface Test Date

**Step 2:** The federate developer submits a conformance notebook via the web site for the Federate Under Test (FUT). The conformance notebook consists of the following, i.e. a Simulation Object Model (SOM), a Conformance Statement (CS), and optionally, a Scenario File. The Certification Agent (CA) conducts three tests on the SOM and CS. They are the CS Dependency Check, the SOM Parseability Test, and the SOM/CS Cross Check. The CA will notify the FUT that they have either passed the three tests or have problems. Once the FUT passes Step 2 they are notified to proceed to Step 3.

**Step 3:** Submittal of interface (IF) environmental data. In preparation for the IF test the following information is requested, i.e.

- FOM (.fed file)
- RTI Configuration File (RTI.rid file)
- API, Hardware, and Operating System used
- RTI Execution hostname and Internet (IP) address
- Federation Execution hostname and IP address
- Whether or not a firewall is in place
- Additional Comment Section

**Step 4: Interface Specification & Reporting.** The IF Test requires the FUT to demonstrate every service and SOM capability in the predetermined test sequence, which is designed to represent a subset of the complete capability of the FUT. The final part of Step 4 is the After Action Review (AAR) and paperwork to document the federate's certification of compliance with the HLA. The IF Test has two parts: the Nominal Test, which ensures that the FUT can invoke and respond to all services for which it is capable, per its CS; and the Representative SOM (RepSOM) test, which ensures that the FUT is capable of invoking and responding to services using a range of data contained in its SOM. The Federate Certification Agent will log service data from the test, analyze the data, generate results, and return a Certification Summary Report (CSR) to the federate developer. The CSR is the official record of HLA compliance for the specific version of the federate code tested.

The final part of Step 4 is the AAR and submission of the SOM to the HLA Object Model Library (OML) is also required before receipt of the Certificate of HLA Compliance. The Object Model Resource Center (OMRC) has replaced the OML.

## 2.2 Required Resources

The resources required for federate testing cover human, software and hardware aspects. These are covered in more detail in the following sections.

### 2.2.1 Human Resource Requirements

To conduct federate testing there is a minimum of one person required to resource this process, i.e. the Certification Agent (CA). However, in order to support all administrative issues associated with federate testing it is recommended that this process is resourced by at least two (2) people. There is also a need for additional office and information technology (IT) support. With reference to the CA the requirements for this role are listed below, i.e.:

- Must have an understanding of the HLA specification and the interpretation of the specification.
  - Example: requestFederationSaved: A federate which initiates a federate save must handle the save process.
  - requestFederationSaved =>initiateFederateSave
- Must have a working knowledge of networking
- Must have an understanding of those operating systems that support RTI implementations
- Must have an understanding of programming
- Should have some simulation background experience

### 2.2.2 Software Requirements

There are two main applications that are required in order to establish a federate testing capability, i.e. the Federate Test Management System (FTMS) and the Federate Compliance Testing Tool (FCTT). The FTMS is a Web-based system for administering federate testing. The FCTT performs pre-runtime file checks as well as runtime tests.

The FTMS process begins with a candidate federate's application for testing, and continues with the uploading of required test documents (e.g. SOM and CS) and the specification of key test information (e.g. test environment, security restriction, and contact information for the certificate). Since the early development of the FTMS this system has been significantly revised to take advantage of new developments in Web technologies and computer hardware. As a consequence FTMS v2.0, is implemented via Active Server Pages residing on a Windows NT 4.0 server running Internet Information Server 4.0. FTMS v2.0 features a simplified user interface leading to improved usability and shorter page download times, an improved administrator interface for use by the CA, and an internal architecture designed for more efficient long-term maintenance. Compared to previous versions the FTMS v2.0 system saves operating costs and improves the overall test process.

The HLA FCTT joins a federation and monitors HLA federates. The data obtained by monitoring the executing federates is compared with the respective federate SOMs and their conformance statements to determine if the federate properly fulfills its responsibilities. The FCTT was developed as an extension to the Federate Verification Tool (FVT), which is an application which joins a running federation to monitor federate activity, but in a more general way than FCTT. The FVT tool was written in Java to enable multi-platform support without requiring specific developer action for each hardware platform type, operating system, RTI vendor, and RTI version. As a result the FCTT is also a Java application. Furthermore it should be noted that the RTI version must be verified in accordance with the DMSO verification process.

In addition to the FTMS and the FCTT, the minimum underlying software requirements needed to support this process and associated tools are specified below, i.e.

- Microsoft (MS) Windows NT 4.0 Server & Service Packs to 6
- MS Windows NT Option Pack 4.0
- Web services
- Simple Mail Transfer Protocol (SMTP) services
- Posting Acceptor
- Supporting Applications:
  - MS Access (MS Office 2000)
  - Text Editor of some kind for the Tools
  - Front Page 2000 is optional

### 2.2.3 Hardware Requirements

With respect to computer hardware issues the minimum set of requirements needed to support the FTMS process and FCTT are specified below, i.e.

- Personal Computer (PC Server) Minimum Requirements:
  - Microprocessor frequency: 400 MHz
  - 256 Megabytes of Random Access Memory (RAM)
  - Hard Drive: 8 Gigabytes
  - Compact Disk (CD)-Read/Write Device
  - LAN Internet Connection

**This page has been deliberately left blank**



**Page intentionnellement blanche**

## Chapter 3

### 3. National requests and positions on HLA certification

#### 3.1. France

France has been developing distributed simulations since the early 90s, using DIS and ALSP standards, and more recently the HLA standard for constructive and virtual simulations.

While several legacy systems are still relying on DIS, HLA is now widely considered – more or less formally - as a necessary standard for new simulation systems. Notably the HLA was officially chosen in March 1998 as the standard for joint simulation (at strategic and operational levels) as well as for Air Force simulation systems in 2000. In the acquisition area, depending on the Délégation Générale pour l'Armement (DGA, the French procurement agency), it's the keystone of models and simulations reusability and thus a major element of the simulation based acquisition policy.

There are currently many HLA based activities in France aimed at developing HLA expertise and providing HLA compliant simulation systems for the joint staff, armed forces, and the procurement agency. As an example the ALLIANCE Joint CAX Project was started in 2001, which could also provide the basis for contributing to the NATO Pathfinder Programme. One of the main concerns of these ongoing developments is how to validate delivered simulation systems according to HLA conformance requirements. To date, there is only one HLA-certified federate, i.e. ESCADRE/ELYSA, which is a constructive simulation for analysis. The US DMSO certified this federate application in June 2000. In the future however, many simulations will require testing, and a national HLA certification capability appears to be necessary. The Joint Staff M&S Action Plan (1999) has identified this requirement as an action item.

Further, as more and more simulation systems will be used in multinational federations, the certification process should be coherent with our allies' process, especially within NATO. To ensure that coherency and to develop a national HLA certification capability in the most cost effective way the favoured solution is that France participates with other NATO countries towards the development of a HLA certification process and tools for NATO. This participation may include a mix of funding, human resources and facilities to host certification activities.

#### 3.2. Germany

In 1999 the German Procurement Agency (BWB) established a center of expertise at its Technical Center for Communication and Electronics WTD 81, Greding. The corresponding section called *Simulation Architecture and Infrastructure*, launched a concept for a so called *Proposed Standard Interface for Simulation Applications*  $\Psi$ -SA, and has become a national focal point for future HLA-related R&D activities in Germany.

$\Psi$ -SA represents an external view on the capabilities of a simulation component in terms of an object space and specified operators, which is best performed by strictly using object oriented analysis and design methods. In some sense,  $\Psi$ -SA becomes the object-oriented extension to the HLA based on a “model-driven” view on a scenario – in contrast to a data-structured view. With this at hand  $\Psi$ -SA induces the process of adding semantic aspects by means of its specific methodology.

With respect to its layered architecture  $\Psi$ -SA incorporates the HLA-OMT on the one hand (as a lower level representation of a federate) and the HLA Interface (IF) Specification without reference to any specific RTI. The lowest layer of  $\Psi$ -SA encapsulates the HLA IF Specification in an object-oriented manner and becomes the generic key to any (private) so called *RTI-Socket Implementation*. To this date, several RTIs have been extended by their corresponding RTI-Sockets to easily being plugged into the  $\Psi$ -SA architecture (e.g. DoD-Suite of RTIs, MäK-RTI, Pitch RTI, German RTI based on CORBA).

The concept and the corresponding prototype implements the vision of a low cost technical infrastructure, which comprises semi-automatic HLA-certification, and modeling methodology based on state-of-the-art

technologies (object orientation, UML). This approach avoids imposing any restrictions on the choice of an RTI and offers a maximum flexibility to the modeling process. The underlying architectural boundary conditions help to separate responsibilities in terms of reliability of

- the model and its corresponding simulation application (the simulation model proponent)
- the software layer to adopt  $\Psi$ -SA (the SOM proponent)
- $\Psi$ -SA itself (owned by MoD, maintained by contractors)
- the RTI-Socket layer and the corresponding RTI-implementation (the RTI proponent).

Especially the HLA-certification process applies to each federate separately. The federate development decomposes into the steps as being induced by the architectural boundary conditions:

- Create the simulation model and its SOM
- Adopt the  $\Psi$ -SA interface according to the SOM and FOM ingredients
- Make a choice for an RTI and its  $\Psi$ -SA compliant RTI Socket implementation

After being approved by MoD SMEs, HLA-certification of the federate appears only to be a small step having in mind a successful certification of the  $\Psi$ -SA infrastructure including the suite of available RTI sockets (transitivity argument).

### 3.3. Poland

Poland aims to realise the NATO goal EG 0350, which is connected with the development of simulation systems for CAX and support to operations.

Polish Armed Forces decided to build the Centre of Simulation and Computer Wargames. The centre has just started this year and will be equipped with many simulation systems and among others will be equipped with Joint Theatre Level Simulation (JTLS) and national simulation systems for supporting a range of exercises (i.e. corps-division-brigade level).

The operational requirements for the national simulation system specify compatibility with NATO systems. The communication and synchronisation requirements will be realised with HLA standards as described in an official document (confirmed by authorities).

The national simulation system is scheduled to be completed by the end of 2003. The precise operational and technological requirements and conceptual project were prepared in 2000. Currently the technical activities are being implemented based on the FEDEP and the HLA Rules. The compatibility and interoperability of Polish simulation systems require the justification for HLA certification.

In Poland there are many centres where simulation systems are developed. One of them is the Faculty of Cybernetics in the Military University of Technology, which takes part in the realisation of NATO goal EG 0350. Many scientific and research projects connected with interactive and distributed simulation for exercises and combat analysis have been developed since the early 1990's, using different protocols, own ideas, DIS and finally HLA.

To date, a Distributed Interactive Simulation Environment (MSCombat) has been constructed and developed for Computer Assisted Exercises (CAX) and Decision Support Systems (DSS):

- Division-Brigade-Battalion levels
- Editors for scenario development
- Constructive simulation + VR components
- Mathematical combat models for battalion level
- Artificial Intelligence components
- Object-orientation
- Heterogeneous environment (hardware and software)

Currently MSCombat is being developed to represent a larger scale synthetic environment based on the HLA and implemented using RTI 1.3 NGv.3. The software interface has been developed using the MODSIM language. This interface provides communication and synchronisation services as a broker between the RTI and Polish federates, MSCombat (regulating federate), graphical editors (constrained federates) and databases.

In conclusion, Poland is keen to take part in multinational federations within NATO and would therefore be willing to participate with other NATO countries towards the development of a HLA certification process and tools for NATO.

### 3.4. UK

In recent years the role and potential of Synthetic Environments, Modelling and Simulation (SEMS) to support UK Defence programmes has expanded dramatically. This expansion is highlighting a number of issues that need to be resolved to enable the full potential of larger scale Synthetic Environments (SEs) to be realised and exploited. These issues centre on the need that credible SEs can be designed and developed in a cost effective manner, based on the integration of verified M&S components, and the capability to interoperate with other systems to support national and international exercises, e.g. NATO. In this context the UK MOD will aim to maximise, subject to defence constraints, the reuse of SE infrastructure, components (models, simulations and data) and services across applications, through the adoption of effective information management techniques, common frameworks, processes and standards. The creation and management of some form of SEMS repository or Shared Data Environment (SDE), set up to capture qualitative and quantitative information will form an essential part of this initiative.

Within the UK SEs are already used widely in military training, e.g. Combined Arms Tactical Trainer (CATT), Medium Support Helicopter Aircrew Training Facility (MSHATF), and the business case for their use within the UK has been defined and accepted for some time. Within newly expanded roles into the areas of campaign planning, mission rehearsal and operational decision support, the case for the use of SEs is equally clear. In all of these cases SEs are now seen as the only cost effective means of achieving the necessary capability.

The Smart Procurement Initiative (SPI), a fundamental part of the UK Strategic Defence Review (SDR), recognises the unparalleled opportunities offered by SE Based Acquisition (SeBA) to support all aspects of its inception and operation. The SeBA concept envisages the use of SEs throughout the whole of the Equipment Acquisition life cycle with particular emphasis on their use in the Concept and Assessment phases. To date, relevant activities include a SeBA Case Study based on Integrated Ground Based Air Defence (IGBAD), the Combat Systems Integration (CSI) Testbed, the FOAS SE Demonstration, and the Joint UK/US Distributed Simulation (JUDS) Project.

Use of 'best practice' is critical to the assembly and use of SEs. This should ensure that a SE is 'fit for purpose', that appropriate systems and components are being linked together and will facilitate better verification and validation. The current 'standard' process that is being developed to support best practice in the creation of SEs (federations) is the HLA FEDEP (Federation Development and Execution Process). The UK MOD Synthetic Environments Coordination Office (SECO) strongly encourages the use of the FEDEP as an underpinning activity for the development of SEMS applications.

SECO recognises that there are considerable issues in policing any policy on SE standards, and consequently supports activities that are currently in place (e.g. within the NATO NMSG forum) to address these issues, including processes to test and verify compliance of federate simulations.

The UK has recognised the need for a National Focus for Synthetic Environments (NFSE) to provide a framework upon which to develop the required set of SE Infrastructure and Services (I&S) including, for example, HLA compliance certification. Means to establish such a focus are being explored in addition to working towards an interim set of services under a temporary focus.

### 3.5. US

The HLA compliance test suite for HLA federates is already in use by models and simulations, both within and outside the US Department of Defense. This compliance test suite is the means by which the



model and simulation owners verify that their policies and guidelines (currently at the US DoD Service level) are fully implemented. Each Service has signed, or at least has in development, policies and guidelines that call for their models and simulations to be 'HLA Compliant'. Furthermore, within the US DoD the HLA is the subject of Service and Agency Memorandum of Agreement (MoA), signed in November 2000 (with no written end date). The MoA calls for the HLA to be the interoperability architecture among models and simulations; and that any other approach to achieving interoperability must be justified.

The US DoD HLA program is undergoing transition. The transition strategy of the HLA program is focused on the consolidation of program resources, the termination of selected elements of the program, the transition of selected program elements, either to commercial vendors or to other organisations within the DoD and finally the retention of those program activities by the DoD that are of interest to the DoD. DMSO will retain the following for the US DoD:

- Federate Certification, RTI Verification,
- Specification Interpretations (1.3 and 1516),
- Repositories. The US participates in multinational federations within NATO and will contribute towards the development of a HLA certification process and tools for NATO.

### **3.6. Summary of national positions**

Nations participating in this task group are France, Germany, Poland, the UK and the US. All recognise the importance of the HLA certification process in facilitating technical interoperability based on the proposed NATO HLA STANAG. The establishment of a NATO certification capability is a desired goal for all those nations. This should be considered as a generic service offered to HLA federate developers to facilitate their integration in future federations and helping to improve their skills in the HLA domain. It should not be considered as a mandatory requirement for every developed simulation application. However this flexibility should not prevent any future NATO programme to require the HLA certification process to be applied prior to federates being integrated within a NATO federation.

Nations participating in the Task Group have identified the need for establishing national certification capabilities. However they recognise that, except in the US, the number of federates to be certified for HLA technical compliance could be relatively small and therefore this would not justify the establishment of a permanent capability within individual nations. Access to a NATO certification capability by nations for their own requirements has been initially discussed within this Task Group. Reviewing these requirements is considered as a prerequisite before national support towards the development of a NATO capability takes place.

Participating nations have raised the issue of a need for a conformance test procedure relating to simulation frameworks. It is recognised that HLA federate developers (problem solvers) are more efficient when using a dedicated and well defined set of processes, frameworks and tools, providing them with easy access to HLA services at minimal cost. To date the DMSO compliance process only applies to federate applications, and a separate process is available for RTI verification. This apparent limited scope of compliance / verification checks raises some concerns about the current compliance and verification process. In the case of development tools and simulation frameworks being HLA certified then, by transitivity this could provide some assurance that federates which are developed based on the corresponding tools and frameworks are inherently HLA compliant. This evolution of the current certification practice is considered as being highly desirable by a majority of the nations and needs to be addressed by a future NMSG Task Group.

## Chapter 4

### 4. Conditions and constraints for establishing a NATO capability

This chapter discusses the conditions and constraints specific to a NATO implementation of a HLA certification capability with respect to administrative and funding procedures specific to NATO. It also describes the relationship of this new capability with some existing organisations or new projects in NATO or member nations.

#### 4.1. Resourcing / funding issues

As it is known, the new NATO M&S organisation was set up in 1998 without providing it with a specific budget for establishing key activities such as the establishment of an M&S Help Desk, HLA certification activity, etc. At present, only a limited budget is made available for providing edition of documents, office work and space, travelling for personnel of the Modelling and Simulation Co-ordination Office (MSCO) and a limited technical support for marketing activities.

In establishing an effective M&S capability or even a demonstration within NATO, the M&S organisation has to follow a very long and specific process to convince authorities to allocate a part of their budget to a new activity. New requests have little or no chance to be considered except if they are strongly supported by high commands. This support is only provided if there is a clear and direct link with operational requirements. In the case of a very technical activity such as the HLA compliance certification, it will be difficult to demonstrate that this activity is directly useful from the operational point of view. This is due to the fact that the people concerned have little or no background in the M&S domain and no idea at all what challenge(s) represents the use of HLA. Military people role is to express operational requirements for example for training or operational support and they do not concern themselves with the technical way those requirements will be solved. Therefore, the traditional funding process has little chance to be successful and even if it is, the timeline would be too long to offer real benefits (See Section 1.4).

Then, until a specific budget dedicated to M&S becomes available, this funding constraint will force the establishment of a HLA compliance certification capability to be either supported by an already existing NATO technical organisation such as NC3A or funded by Voluntary National Contributions (VNC). In the first case, the technical centre has to fund the implementation of this HLA capability as a part of its overall technical infrastructure that is used for developing its technical capability to support military requirements. In the case of a VNC, participating nation would accept such a charge only if there is some advantage provided to increase its own HLA national capability.

#### 4.2. Relationship with other organisations

The HLA certification capability is not independent of other M&S initiatives and capabilities within NATO and/or NATO nations, such as the establishment of an M&S 'Help Desk' or of a Simulation Resource Library. To emphasise this fact, it can be understood that the reuse of simulation resources (a clear benefit from the HLA approach) will never happen unless a repository of certified products is made available to NATO. So the establishment of an HLA certification capability is a prerequisite for an effective M&S activity within NATO. Related or parallel activities are in the process of being established within NATO and it is the responsibility of the MSCO to oversee the internal consistency of the new structure.

##### 4.2.1. US Help Desk

The US DoD established the HLA Help Desk to provide dedicated support to M&S sponsors, users, and developers of HLA. To accomplish this goal, the HLA Help Desk was designed as a central point of contact for all questions regarding the HLA. The HLA Help Desk employs a growing repository of HLA knowledge and the help of the leading HLA subject matter experts to answer all questions relating to the HLA, including HLA Certification and Federate Compliance Testing. By being the central clearinghouse

for HLA questions from the M&S community, the HLA Help Desk is able to save the community, as well as the subject matter expert's time and effort, not to mention the building of an expansive HLA data repository. In order to remain in this role, the HLA Help Desk must continue to be closely tied to the HLA Federate Compliance Testing activity to provide the necessary support to federate developers wanting to become HLA Compliant or in the process of becoming HLA Compliant. As the US DoD continues to maintain the HLA program, the HLA Help Desk will remain a central, integral part of the overall support to the entire HLA community.

#### 4.2.2 Re-use paradigm

The re-use paradigm supported by the HLA is mainly based on the SOM of candidate federates. So the importance of HLA certification for recognising the value of a federate is paramount; the HLA certification activity would provide verified components for a SOM/FOM library with some guarantee that potential federates can be integrated in a new HLA federation in a cost effective way.

For many already mentioned reasons (mainly manpower and budgeting issues), HLA certification and other related capabilities are not established so far within NATO and the US is provisionally offering to use its own organisation at no charge to the NATO and the PfP nations. Even if it is doubtful that the future NATO capabilities mirror exactly the current and future organisation, one can believe that the future NATO organisation will offer a similar functionality. Since the US capability is already developed and is now running for some years, it is a strong requirement that the HLA certification activity not only stay consistent with the other NATO activities, but also with the US ones. In particular, HLA being a standard there is an obvious need that the certification software suite stays unique and is developed from a unique source, which is the current US DMSO suite. If this coherency condition is insured, the transition from a US support to a NATO support will be transparent for other nations. Another advantage for this consistency approach will be the possibility to share development costs between some nations while the current cost is only supported by one nation.

#### 4.3. Reference HLA STANAG

During 2001 a NATO Standardisation Agreement (STANAG) on 'Standardised Modelling and Simulation Information for the High Level Architecture (HLA)' was drafted and recommended for endorsement by the NATO Alliance Nations. This activity was carried out under the responsibility of the Land Group 8, NATO Army Armaments Group (NAAG).

The aim is to facilitate system-level interoperability within and between operational and training systems developed by and located in different NATO nations. This draft STANAG recognises the transitional nature of the HLA from DMSO v1.3 to the IEEE 1516 standard.

Under this STANAG, participating nations shall agree that:

- HLA is not just recognised as an architecture standard, but that there are other related initiatives, significantly the FEDEP system engineering process and the HLA compliance test suite,
- If interoperability is required the relevant M&S systems are conformant to the current edition of the HLA,
- When developing or procuring applicable future M&S systems (e.g. federate simulation) they will be verified in accordance with the HLA compliance test process, based on national requirements,
- Details of national M&S systems that are compliant to HLA are published and made available through an Simulation Library / Repository.

#### 4.4. M&S community awareness

There is an increasing trend in both NATO and PfP countries towards the development of federations to support equipment acquisition and training system programmes.

For example the German military community has spent significant effort in an overarching modeling concept for the GE Armed Forces Services. The idea is to achieve crossover compatibility of communication services with the help of an underlying and domain independent conceptual model. The

technical approach is currently under investigation by the GE Armed Forces Technical Center for Communications and Electronics WTD 81, Greding. The building blocks of the architecture include various Data Interchange Formats and Data Exchange Mechanisms (e.g. a Data Mediation Functionality to bridge between a Common Data Model and several individual data models from C4I components, FOMs and SOMs), and communication infrastructures such as GE RTI based on CORBA (GERTICO), Protocols, Message and/or Replication Mechanisms, Shared Memory. Related activities currently apply to several R&D projects such as the US/GE cooperation on SINCE (Simulation and C2 Information Systems Interconnectivity Experiment), FR/GE cooperation on distributed simulation experiments, and multinational cooperation on distributed simulators over WAN infrastructures.

In France HLA forms one of the key roles within a simulation-based acquisition policy produced in 1999, i.e. fostering reuse of models throughout the system acquisition cycle and the building of more complex and global simulation of systems, i.e. virtual prototypes. The ARCOSIM project which is in progress will define a global M&S common technical framework for the research, T&E centres, which will include HLA as the main standard for simulation applications interoperability. The HLA adaptation of the ESCADRE simulation support environment (dedicated mainly to analysis) and the certification in June 2000 of the ELYSA federate, based on that new version of ESCADRE, can be considered as a first step towards the achievement of ARCOSIM goals. It is also worth noting that the French Joint Staff and the Air Force has made HLA mandatory in their M&S area. The Army has a requirement for the HLA to form part of its most important Staff Training Programme, and the Navy has developed an HLA framework called RAL (standing for RTI Abstraction Layer) to be used in their simulation projects.

The US continues to raise community awareness on the compliance test suite through SISO Simulation Interoperability Workshops (SIW), participation in NATO M&S working groups, and encouragement of commercially developed HLA products. Other relevant forums include ITEC, the International Synthetic Environment Symposium (ISES) and selected Simulation Conferences and HLA Forums held within participating NATO countries. Additionally, the previously referenced MoA for US DoD serves as a basis for the use of HLA compliant federates within the DoD. Information about the test suite can also be found at <http://hlatest.msiac.dmsomil/>.

Within the wider NATO M&S community there is a clear need to increase the awareness of the existence and use of the HLA Compliance Test Suite. This should be accomplished by member nations through increased participation in the various M&S Conferences and Workshops as described above. It is also recommended that Member nations should include contractual requirements for the HLA compliance testing process to be included in contracts which involve the development of M&S assets.

## 4.5. Partnership for Peace issues

Co-operation on PfP began in 1990, when NATO and the former Warsaw Pact nations signed a Joint Declaration stating that they no longer regarded each other as adversaries. In December 1991, the North Atlantic Co-operation Council (NACC) held its first meeting. Confidence building activities such as the sharing of information and observation of exercises took place under the auspices of the NACC, but a need was soon expressed to set up a structural framework for the practical, defence-related and military co-operation activities. In January 1994, NATO invited the NACC and the Organisation for Security and Co-operation in Europe (OSCE) countries to join a Partnership for Peace (PfP).

The main objectives of PfP are:

- Facilitating transparency in national defence planning and budgeting processes,
- Ensuring democratic control of defence forces,
- Maintaining the capability and readiness to contribute to operations under the authority of the UN and/or the OSCE,
- Developing co-operative military relationships with NATO to undertake missions in peacekeeping, search and rescue, and humanitarian operations,
- Developing forces that are better able to operate with those of NATO.

PfP is a practical program, with NATO working in concrete ways with each Partner towards greater transparency in defence budgeting, aimed at improving civil/military relations and promoting democratic

control of armed forces. Through joint planning and joint exercises the program helps to develop the ability of the forces of partner countries to operate with NATO forces in such fields as peacekeeping exercises, search and rescue and humanitarian operations. The non-NATO PfP members are:

Albania, Armenia, Austria, Azerbaijan, Belarus, Bulgaria, Croatia, Estonia, Finland, Former Yugoslavian Republic Of Macedonia (FYROM), Georgia, Ireland (Eire), Kazakhstan, Kyrgyz Republic, Latvia, Lithuania, Moldova, Romania, Russian Federation, Slovakia, Slovenia, Sweden, Switzerland, Tajikistan, Turkmenistan, Ukraine, Uzbekistan.

In 1998, the U.S. took the initiative to implement a series of Computer Aided Exercises (CAX) involving the PfP Nations. On November 18th in the same year, the U.S. signed a MoU with Sweden about the provision of PfP CAXs. Sweden then hosted one of the largest CAXs ever held, i.e. the PfP Exercise Viking 99. Subsequent to this exercise the PfP objectives over the following 3 years are outlined as:

- Improve/standardise modelling and simulation capability (HLA included),
- Publish minimum requirements for communications technology and demonstrated systems architectures,
- Develop a mechanism for scheduling, planning, and conducting exercises,
- Identify doctrine, tactics, techniques, and procedures for Peace Support, Search and Rescue, Humanitarian Relief, and other PfP agreed operations,
- Co-ordinate technology with defence academies and PfP training centres in common areas such as distance learning.

Within the PfP Nations Sweden is leading activities related to the HLA development process. This includes the development of a commercial RTI, i.e. the Swedish pRTI. The pRTI achieved formal HLA verification for the HLA 1.3 NG Interface Specification. A new version of the pRTI is being developed in accordance with the IEEE 1516 standard.

Most PfP nations are developing M&S capabilities. Establishing an HLA compliance certification capability is not their first priority, since in many cases these capabilities are based on GFE/GOTS and/or COTS based products and tools, i.e. if the application software is provided by NATO countries it should be HLA certified. In other cases PfP requirements for HLA certification testing should be supported by NATO or a NATO nation.

## 4.6. Test Suite enhancement issues

This section will address two types of enhancement issues. The first issue is associated with software upgrade/maintenance aspects and the second issue is relevant to how the compliance test suite is utilised with respect to middleware and federation testing.

### 4.6.1 Software

The DMSO compliance test suite needs to be enhanced to maintain currency with the evolving HLA standard, e.g. the capability to support both the DMSO v1.3 and the IEEE 1516 standard. The test suite must also be able to handle other RTI implementations in addition to the DMSO RTI 1.3NG. Further enhancements will be identified by member nations to DMSO upon their implementation of the compliance test suite.

### 4.6.2 Increased testing scope

The DMSO Conformance Test as outlined above requires at least two HLA-relevant information contents to be supplied by the Federate Under Test FUT:, i.e. the SOM and the Conformance Statement CS.

The CS provides the functional interfaces to the CA being necessary to communicate the FUT's SOM contents properly. The DMSO compliance test suite passively records any function invoked by the FUT. Since the CS is to be delivered by the SOM proponent it seems that at this level of information, the FUT's conformance test shows some limitations. The subsequent set of paragraphs attempts to discuss some of these issues.

#### 4.6.2.1 GENERAL ISSUES FOR DISCUSSION

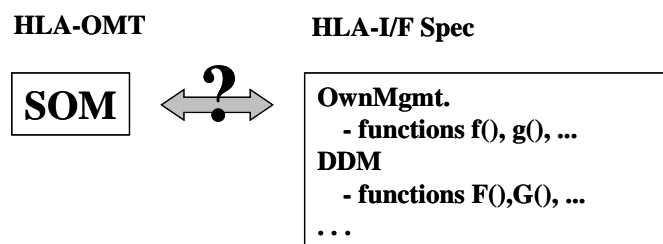
The general question which arises is: *What is the definition of HLA Compliance from a general point of view in accordance with the FUT's SOM?* If we limit ourselves to a certain level of syntactic interoperability we claim that the FUT should be able to at least

- reflect objects based on subscription
- reflect receipt of interactions based on subscription

The publication of objects and interactions is already covered by the DMSO compliance test suite. As a consequence, the test suite would need to be extended to provide an enhanced FCTT which is capable of stimulating federates, thus incorporating the essential capabilities to send necessary information to the FUT and thereby analysing its behaviour in terms of stability and limited functionality, e.g. destruction of objects upon receipt of certain kinds of interactions.

From this general observation another question arises, i.e. *To what extent could the CS be predefined based on the SOM only?* It is expected that to a certain degree the CS may be defined based on its SOM and according to the HLA I/F Specification, e.g. any publish, update, subscribe and reflect mechanism to be invoked by the FUT.

On the other hand, certain mechanisms cannot be derived from the SOM, e.g. Time-Management capabilities of the FUT.



As long as some kind of “Guidance, Rationale and Interoperability Modalities” (GRIM) document does not exist this will result in a lack of information which can be captured. However, it is up to the FUT proponent to fill this information gap by a FUT-specific CS.

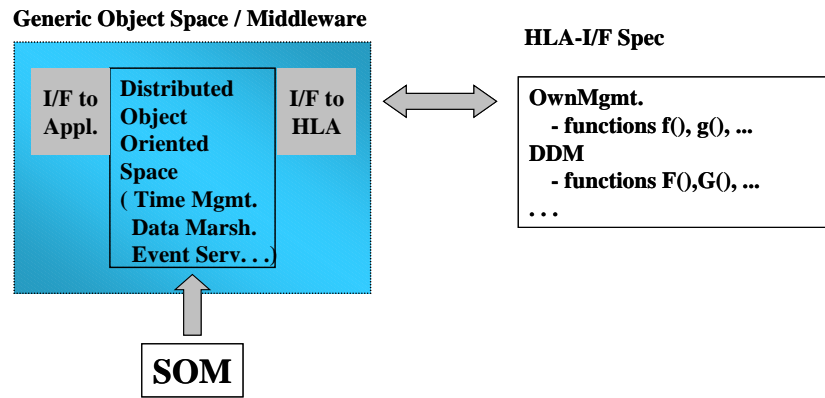
Consequently, it is suggested to divide the former CS into a SOM-dependant part (i.e. the generic CS), and a FUT-specific part.

#### 4.6.2.2 MIDDLEWARE ISSUES

In order to avoid uncertainties related to whether the FUT fulfils its requirements of being HLA compliant, one possible solution is to rely upon a generic (i.e. FUT independent) interface to the HLA RTI, which completely encapsulates the HLA interface in order to make this available to any federate application. This aims to achieve HLA-compliance by separating the application, i.e. the SOM implementation, from the HLA-interface by an appropriate layer of generic middleware.

If this middleware layer could be approved to be HLA compliant in terms of the HLA interface it would be up to the FUT developer to apply those functions properly.

Using this approach there is more potential benefits to the M&S community. Specifically, a generic concept on a distributed and object oriented simulation space would significantly help to specify how objects and events in space and time behave and are to be matched to the existing HLA interface standard, i.e. for effective support of HLA conformance testing, there is need for an object oriented extension of the HLA-OMT:



#### 4.6.2.3 PROVISIONAL CONCLUSION

The previous set of paragraphs (i.e. Paragraphs 4.6.2.1 and 4.6.2.2) provides some typical examples of ideas which could be addressed when discussing future improvements of the HLA certification compliance process. Some other ideas may be raised in the course of future HLA developments.

Paragraph 4.6.2.1 deals with what can be considered to be HLA Compliant. Paragraph 4.6.2.2 deals with the use of middleware. Middleware has been and will be a continued use by federate developers to assist them in the implementation of the HLA Standard for their federates. Currently, the US DoD will not certify a middleware application alone as being HLA compliant. This is a policy decision; although each member nation could test a middleware application linked to a generic federate and certify that it is complete. This would have to be all inclusive (i.e., handle ALL the RTI services) and would just use any SOM that defined all the possible capabilities as an absolute minimum.

Another issue raised is federation testing. The FCTT can test multiple federates as the federation is running and provides results for each federate; nevertheless there is no determination that the federation as a whole is compliant.

These issues require a review of what it means to be HLA compliant. Currently to be certified as HLA compliant a federate must demonstrate its adherence to the three specification documents defining the HLA: the HLA Rules, the Interface Specification, and the Object Model Template Specification. The development of the federate compliance test process was guided by a few specific principles. The first was that HLA compliance would require demonstration of technical interoperability only, not substantive interoperability as discussed in an earlier paragraph. That is, certification of HLA compliance in and of itself does not automatically mean that a particular federate is suitable for a particular federation.

Another guiding principle for federate compliance testing was that the tests should require as little additional work for the federate developer as possible. Some documentation, such as the SOM, is required by the HLA specifications, but additional documentation not specifically required by HLA is deliberately minimised and simplified wherever possible. The CS, for example, can be filled out in any text editor by editing a sample CS.

Exhaustive testing, where the federate would be required to demonstrate every capability (possibly hundreds or more) indicated by its SOM, was rejected as an unnecessary burden for the FUT. Instead, the FUT is asked to demonstrate a representative subset of the capabilities indicated by its SOM. For example, if the FUT's SOM indicates that it can update a large number of different attributes, the FUT is asked to demonstrate updating at least three specific different attributes.

It is recommended that these issues should be addressed further, for example in a future NATO M&S working group.

## 4.7. Security and proprietary information issues

Three components of a federate can be a source of concern related to security, i.e.

- The models, which are more or less accurate representations of real world systems, in particular with respect to system behaviour; this means that these models can potentially have the same level of classification as the real system,
- The data describing the system, which is usually an input to the corresponding model; this data contains valuable and sensitive information about the system, e.g. the range of detection for a sensor,
- The design of the federate itself which may incorporate company proprietary information,

If a model or any part of its supporting documentation (e.g. SOM) is classified, then it cannot be certified remotely through the Internet. It must therefore be tested either using a specific MoD classified network or at a classified (remote) site. In either case the appropriate administrative issues will need to be addressed (e.g. security clearance); in addition, certification at remote site will require the CA to install a local version of the test suite (e.g. from a CD-ROM) on a computing resource provided by the federate developer. This means that in the case where nations do not have any certification capability they will have to address relevant administrative issues or develop their own certification capability.

When the only classified part is the data (not including the SOM), it is still possible to supply unclassified data for testing purposes, provided that its design allows this operation (i.e. no classified data embedded in the code). This has been done many times within the US testing environment and in multinational distributed simulation experiments.

Even if it is expected that a large number of federates will be unclassified the impact of handling classified material must be considered by nations when establishing their position about HLA certification.

Another source of problem that can be related to security issues is the inability to open communication ports directly between the CA site and the federate site. This is typically the case when a corporate firewall and global information systems security policy does not allow the required ports to be opened. Again, in this case, either the certification must be done locally or the federate moved to another site.



**This page has been deliberately left blank**



**Page intentionnellement blanche**

## Chapter 5

### 5. Different implementation hypotheses

#### 5.1. Permanent NATO certification centre

##### 5.1.1. Location

According to the US experience, a facility to be selected for the implementation of the HLA certification activity need not be very large. The main requirements being:

- A small team of two or three experienced people,
- An Internet connection using a professional Internet Service Provider (ISP),
- An appropriate set of PC equipment

Finding some suitable accommodation within NATO should be easy, but having a permanent technical support of computer scientists for networking and operating system issues is also required, in addition to the specialist team concerned with the HLA certification activity. Current NATO facilities are well equipped with networks and computers, but due to the specific technical nature of the HLA activity it would better to host it within a technical agency. For this reason, only two locations seem possible, i.e. the Research and Technology Agency (RTA) in Neuilly (France), and the NATO Command Control & Consultation Agency (NC3A) based in The Hague (The Netherlands). Both locations have good accessibility and international transport connections. Other NATO agencies are less suitably located and do not have a general activity in the M&S domain. There is also another issue to consider, and that is both agencies are located in Europe and this can be shown as a negative aspect for North American nations, for time difference and cost reasons. This remark will be considered further in the final discussion of this solution.

##### 5.1.2. Funding

The initial costs to resource the facility would be required for acquiring and supporting hardware and software, i.e. PCs, specific materials for networking connection (internal links, routers, bridges, etc.), initial subscription and connection to a reliable ISP. Acquired material should be of high quality; for example, PCs need to be powerful and fitted with large RAM and high capacity hard disks. Maybe the selected agency can take a part of this acquisition on its own equipment budget or reuse a part of its already existing devices.

The human resources could be either NATO personnel or hired staff from an industry company (i.e. contractors). In the second case, the team shall be supervised either by a NATO personnel/office or by a Voluntary National Contribution (VNC). That requirement reinforces the proposal to locate the activity in a NATO facility such as the RTA or NC3A. In both cases (NATO personnel or VNC), a specific budget has to be allocated. Finding NATO positions or hiring extra personnel will raise some NATO administrative issues. This forces the issue of selecting the right personnel, a task which should not be underestimated in terms of delay and workload. Hiring private personnel would facilitate the selection of technical staff, but it would involve more direct costs and would force the initiation of the administrative process of contracting the right company using an international Request For Proposal (RFP), etc.

After the preliminary investment period, permanent funding will be required to cover staff or company costs, updating office hardware and software, updating the HLA conformance testing suites, and maintaining connections to appropriate data and voice networks.

Even if the amount of money to be found for supporting this activity does not appear to be high, it should not be underestimated.

Continuous additional support for this activity is mainly composed of technical support for computers and networks, teleconferencing and a limited capability to travel when remote testing is not possible for practical or security reasons (see following paragraph).

### **5.1.3. Working conditions**

The HLA certification organisation cannot work as a stand-alone one. As already mentioned in paragraph 4.2, this activity needs to be consistent with the already established US activity. There is a strong requirement to establish a permanent co-ordination process between the NATO responsible organisation, i.e. NMSG/MSCO and the US DMSO. That means a common document policy (a Memorandum of Understanding or MoU) on HLA certification has to be agreed upon between NATO, PfP and NATO nations and in particular, the US as the leading nation.

This MoU document will:

- Agree on the use of a unique suite of testing tools,
- Define the agreed HLA versions,
- Describe the decision process and specify the conditions for migrating between different HLA versions,
- Establish the work share,
- Define the funding process and mainly its scheduling,
- Establish priorities and conditions for accessing the HLA certification capability by NATO and PfP nations for common or national purposes,
- Etc.

The configuration control of the testing suite should be common between the US and the NATO activities.

Travelling of relevant staff either from the NATO HLA conformance testing team or from the Federate under Test (FUT) team should be provided by the nation originating the FUT. This travelling fund should in every case be limited by the preferred use of teleconferences or, more generally, of the Internet technology.

### **5.1.4. Use of the NATO facility to meet national requirements**

Some nations recognise that even when not requiring a national capability to provide HLA compliance for simulations, they are interested in requiring this capability for some applications (mainly in the training domain). For those nations, these national requirements would probably not generate an annual level of activity justifying the implementation of a national centre. However, the M&S US internal activity or the joint activity generated by NATO M&S and non-US nations together should create a workload sufficient to justify the establishment of a certification centre.

Since it could not seem sensible for nations (except the US), to establish and run such a capability nationally, the possibility of accessing a NATO HLA certification capability for national requirements shall be considered. It seems obvious that those nations which voluntary support the development of the NATO activity should have an access to the certification process according to a priority which will depend on the availability of the facility, e.g. on busy periods, highest priority should be given to proper NATO activity. Nations not participating in the establishment or the running of the HLA certification activity (either NATO members or PfP nations) could access the facility for specific national requirements with a lower priority.

### **5.1.5 Provisional conclusion on the establishment of a permanent NATO capability**

If this NATO solution is selected, it would be better to establish not one but two certification centres: one in America, one in Europe. An American node already exists, established within the US DMSO. DMSO

is already providing HLA certification at no charge for the NATO community. The US HLA certification facility can support Canadian requirements more cost-efficiently than a European node. In any case, a close co-operation between both US and NATO organisations is required (see paragraph 3.2 and 5.1.2.). Therefore, a clear work share and some integration of both DMSO and NATO capabilities appears to provide an optimum solution, if taking into account the US constraints from the political and practical point of view. Access to the NATO certification facility by nations to meet their own requirements is a prerequisite for nations in order to support this solution.

About the choice of the second NATO location in Europe, both hypotheses of implementation seem sensible. Due to the technical nature of the activity, the expertise and the large involvement of NC3A in the M&S activity, the NC3A selection could be preferred: RTA is mainly an administration agency and, at first glance, doesn't seem to be so appropriate to host such an activity. But, considering the practical requirements, an RTA based capability cannot be fully rejected.

In both the NC3A and the RTA no funding or personnel was made available for this activity so far. From the political and administrative points of view the difficulty to establish such a new activity seems equivalent in both contexts. Considering the technical nature of this activity the NC3A location should be slightly preferred.

## **5.2. Rental of National US certification capability by NATO**

### **5.2.1. US policy on future capability**

Currently the US provides the HLA compliance test suite, and plans are for it to continue as a service available to the M&S community. Typically the service is provided over the Internet, and other supporting mechanisms such as scheduling and after action reviews (AAR) are conducted via email and telephone. The federate under test (FUT) provides the software, and any associated labour and travel for its supporting infrastructure and personnel. Since the HLA is currently the subject of a MoA among the US DoD Service components, and additionally, is the subject of US DoD Service policies and implementation guidelines, it is planned that this HLA Compliance service will continue in its current form. Indeed, it is in the process of being upgraded, both in terms of automated capability, and in terms of migration to the IEEE 1516 HLA Specifications.

### **5.2.2. Description of capability and assessment of costs, prioritisation of requests**

Testing is performed under the Modeling and Simulation Information Analysis Center (MSIAC), contract number SPO700-99-D-0300, as a Technical Area Task (TAT). Under this contract, there are no fees for customers when they apply for HLA compliance testing. The MSIAC currently has two individuals assigned to the task, a Testing Manager and a Certification Agent (CA). The CA conducts compliance testing, and maintains the testing database. The Testing Manager conducts all after action report interviews, prepares required reports and can, if required, provide back up testing capability for the CA.

Under the MSIAC contract there are two methods for obtaining services from Illinois Institute of Technology Research Institute (IITRI). They are the TAT (see Annex A) and a subscription account (see Annex B).

### **5.2.3. “Do nothing” option**

The US Defense Modeling and Simulation Office (DMSO) currently provides the HLA federate compliance test on a no-cost basis for those who request it. Nevertheless, travel and shipping costs may be incurred by the federate under test if conditions do not permit testing to be conducted on-line over the Internet, e.g. due to network technical and/or security issues; it should be noted that these costs may be substantial. In addition, the US DoD currently makes no provisions for any special needs which may be required by non-US federates to achieve compliance.

It is planned that this compliance test capability will continue for as long as HLA is the selected architecture for interoperability by the US DoD Service components. However, there is no guarantee that this service will be made available on a no-cost basis in the future.

In the absence of any future NATO certification capability the administrative aspects of gaining continued access to the US facility should not be underestimated in terms of cost, workload and time. Future support may need to be covered by specific contractual arrangements or via bi-lateral and/or multi-lateral Exchange Agreements between the US and other NATO and PfP nations.

#### **5.2.4. Perception issues**

To rely only on the US for a HLA certification capability means that a skilful team would be available immediately at a relatively low cost, but this also raises some concerns.

First, it would create a dependence between NATO nations' simulation industry that could be wrongly interpreted, especially when the issue of security is considered. Whatever solution is chosen for the NATO certification capability it must address the problem of certifying national classified simulations, which would require security procedural issues to be addressed if conducted by a foreign team.

In addition, if the US was the only country which was capable of deciding which simulation deserves a HLA compliance certificate, this could be perceived as HLA being under sole control of the US community. It is essential that the HLA needs to be recognised as an independent and open standard. This is particularly relevant considering the fact that the current US certification process was initially designed to support the US DoD simulation policy and in the future this may diverge from NATO or national policies.

It is therefore perceived that the use of US HLA resources would require a great deal of communication targeted to non-US simulation stakeholders, as well as proof that their needs and constraints are, and will be considered. As an example this would include a concerted evolution of the US HLA certification process and/or the participation of non-US technicians in the US certification team, so that although the process is located in the USA, it would not appear to be controlled by the US DoD.

In summary, using a US HLA certification facility for NATO is possible, but this may not be well-perceived by non-US simulation stakeholders if some appropriate marketing and technical actions are not undertaken to prove the openness of this process.

### **5.3. Establishing a NATO capability voluntary supported by NATO nations**

#### **5.3.1. Description**

As stated earlier in Paragraph 4.1 the establishment of a NATO capability can raise difficult administrative and/or practical issues. Since nations will have to support the largest part of the cost (even indirectly via NATO funding) if they really want to use the capability for their own purpose, it is sensible to consider the hypothesis of the establishment of a certification capability by a group of co-operating nations. This solution is possible using the process of an official Memorandum of Understanding (MoU) between those participating nations and can be initiated with or without NATO. The only issue with this solution could be the lack of a "NATO label" on the service provided.

This capability could be located in multiple nations (at least two), being hosted within respective national technical centres or other types of organisations, since the remarks of Paragraph 5.1 about practical conditions remain valid. In this situation at least one of the locations would be located in the US with the others being located in Europe. In the case of national capabilities within Europe the hosting nation would be expected to provide the technical support, including relevant personnel in charge of the certification process, as a free Voluntary National Contribution (VNC).

This solution can offer a larger choice of European locations (in theory) than the previous one, as far as many nations are interested in this activity. Potential locations for providing national capabilities are identified as being one of the Paris MoD technical centres (France), the Armed Forces Technical Centre for Communications and Electronics (WTD 81) at Greiding (Germany), the Faculty of Cybernetics in the Military University of Technology in Warsaw (Poland), the Defence Science & Technology Laboratory (Dstl) in Farnborough (UK), and a Dutch technical centre such as FEL TNO close to NC3A. It should be noted however, that the Netherlands have not participated in this technical activity. With respect to this

solution it is important to recognise that close coordination needs to be provided with the MSCO in Neuilly (France).

### 5.3.2. General Conditions

As suggested in the previous paragraph, a nationally supported solution could result in a loss of capability for NATO. The solution to avoid this drawback is to include some NATO participation and coordination in the certification process (by MSCO or NC3A).

As previously mentioned, the certification activity has a serious impact on the re-use capability of resources within NATO. The solution aimed at the distribution of this technical activity within multiple nations does not mean that it is disconnected from other NATO activities such as the Simulation Resource Library (containing information on HLA Object Models), or the future Help Desk.

The US experience has demonstrated the importance of recording testing information and statistics concerning this activity for the evolution and the improvement of the overall process. The technical process can be distributed or located nearly everywhere, but the monitoring, the recording of information and the recognition of HLA compliance should be the responsibility of a NATO centre in close co-operation with the national technical centres responsible for the certification technical activity.

Funding of this activity will be shared between nations without requirement to NATO central funding. This fact and other practical considerations need the establishment of a MoU. The content of the agreement will be similar to the MoU discussed in paragraph 5.1. but in addition it will include the share of responsibilities between nations and how the funding will be provided. All Information Technology (IT) resources, technical support and staffing would be provided by nations either as VNC or as funding contribution.

Ensuring and maintaining consistency and a core level of capability does not raise any supplementary issues when compared with a “pure” NATO solution. The same remark applies for coordination with other non contributing nations (NATO and PfP), with respect to issues associated with networking, travelling fund, maintenance and upgrading the certification testing suite and configuration control issues.

### 5.3.3. Provisional Conclusion

This solution offers the benefit of avoiding the long and difficult process of requiring central NATO funding. It will not avoid the requirement to establish some kind of agreement between nations, but supporting a NATO solution will also need one. This solution will provide associated nations with better accessibility than would be provided with a “pure” NATO implementation.

## 5.4. Solutions’ assessment

The 3 proposed solutions are:

- Establishment of a permanent NATO certification centre,
- Rental of National US certification capability by NATO,
- Establishment of a NATO capability voluntary supported by NATO nations.

These solutions must be assessed by all the nations, using the following set of criteria:

- National and NATO implementation costs;
- National and NATO operating costs, including staff training, i.e. initial training, continuation training;
- Availability of suitable manpower to process requests;
- Availability of suitable certification tools to meet national requirements from each NATO Nation;
- Time required to establish capability, including recruiting and training CA;
- Controllability by nations;
- Conformance to nations’ requirements

- National security;
- National perception;
- Practicability.

<b>Criteria</b>	<b>NATO certification centre</b>	<b>Renting the US Capability</b>	<b>NATO capability supported by nations</b>
National implementation costs	+	++	-
NATO implementation costs	--	++	+
National operating costs	+	0	-
NATO operating costs	--	-	+
Required training	-	++	-
Suitable manpower availability	--	++	+
Availability of certification tools	+	++	+
Time required	--	++	-
Controllability by nations	+	-	++
National security (*)	-	-	++
Meet nations' requirements (*)	+	-	++
National/industry perception (*)	+	--	++
Practicability	0	+	++

(\*) this criterion must be considered as particularly important.

This table should be interpreted as an approximate assessment. It shall be read considering that:

+ / ++ means that this solution seems good/very good according to this criterion,

- / -- means that this solution seems bad/very bad according to this criterion,

0 means that this solution seems neutral according to this criterion.

The NATO capability voluntary supported by NATO nations appears as the preferred solution. The US certification services could be used as an interim solution till full nations' capability is reached.

## Chapter 6

### 6. Conclusions and Recommendations

#### 6.1. Justification for NATO HLA Certification

HLA compliance testing provides a first level of assurance to the federation manager that the federate conducts itself as it says (see paragraph 1.4). Even if HLA certification does not provide a full guarantee of interoperability, it provides the first and necessary step in establishing the future NATO interoperability infrastructure. It will be the first piece of the required technical support that NATO has to provide for future activities. In particular, the HLA certification capability shall provide the best way to populate the future NATO Simulation Resources Library with relevant information, including certified SOMs and FOMs.

Within NATO the HLA was recognised as the preferred M&S interoperability standard in 1998, (see, the “NATO M&S Master Plan”, MSMP). The MSMP was approved at the higher level in NATO, by the CNAD, the MC and finally the NAC. The corresponding HLA STANAG is not yet officially approved, but it is on the right way, the final version of the text being forwarded to the NATO standardisation office in 2001. Nevertheless, no mandatory directive was ever issued by NATO requesting that HLA federates which form part of a NATO federation should be “HLA compliant” certified. However, HLA compliance is clearly mentioned as an important prerequisite in MSMP Sub-objective 1.1 (adopt the HLA as the standard architecture) and MSMP Sub-objective 3.4 (Execute the selected and resourced development strategy). Accordingly, the NMSG decided to examine the possibility of establishing a HLA compliance certification capability within NATO.

This does not mean that the HLA certification should become mandatory, even the NMSG task group does not have the intention to recommend the establishment of an imperative directive signed by any NATO high level authority. However, the task group has the strong opinion that the establishment of a NATO HLA compliance certification process is to be provided as a general and useful technical service to participating organisations in establishing HLA federations.

#### 6.2. Preferred Solution

Following discussions during the task group meetings and considering the numerous issues raised by a “pure” NATO solution, participating nations agreed that the best solution would be to share the HLA certification capability between nations. This solution is described in some detail in Paragraph 5.3. Each nation supporting the establishment of the NATO HLA certification capability would have access to this in the context of meeting national requirements. In this case NATO would delegate the HLA certification of national federates to those respective nations responsible for federate development.

This HLA certification capability must be clearly defined and would be better supported by the establishment of a multi-lateral agreement between nations. The main conditions to be specified in this agreement are described in Chapter 5 of this report. Nations participating in the task group recognise the leadership of the US on this activity and agree on the requirement of establishing a unique testing suite based on the current US software. It is therefore recommended that some joint resources and/or funding needs to be provided by non-US nations participating in this future activity, for maintaining and upgrading the existing testing suite initially funded by the US. In exchange for this, those participating nations will have direct access to the certification software (excluding source code) to meet specific national requirements.

It is recognised that the establishment of a multi-lateral exchange agreement between participating nations will require some years (2-3 years?) to be finalised. Therefore this shared capability would probably not be formally established for at least three years. However, based on the US agreeing to distribute the certification software to NATO nations, the short term solution would be for those nations receiving the software to pursue a process for federate certification outside the conditions of a multi-lateral agreement. The risk with this short term solution would be that information relevant to federate certification testing may not be captured and maintained in a co-ordinated manner across NATO nations. Consequently it is strongly recommended that this issue is addressed by another NMSG working group (currently, the MSG 012-TG 009 “Simulation Resource Library”).



The preferred solution based on the share of capability between nations offers an attractive advantage compared to a “pure” NATO solution, since this avoids the difficult process of securing central funding from NATO. The issue of HLA certification of federates developed by NATO (and mainly the NC3A) has not been discussed due to the absence of an NC3A representative of the task group. Task group members recognise the fact that federates developed by NC3A should offer the same level of guarantee as those developed by individual nations and consequently they should also be subject to the HLA certification process. Therefore some additional work is required to establish how NC3A would be integrated in the overall process. One obvious condition is that NC3A needs to contribute to the discussion of a future exchange agreement as a real partner.

In consideration of those nations which do not provide any form of direct contribution to a shared HLA certification capability they would be able to access such a capability in the context of bi- or multi-lateral agreements with participating nations.

### 6.3. Evolution of the HLA Certification Process

The specific constraints, conditions and requirements for the evolution of the HLA certification process is discussed in detail in chapter 4 of this report. Main remarks are the following. First, it is recognised that the current HLA testing suite shall evolve consistently and in accordance with the evolution of the HLA standard: such a move is currently taking place to evolve from the current US DoD version 1.3 to the IEEE 1516 version.

In fact, the requirements for any particular evolution may have two distinct causes:

- first, a normal evolution of the standard as mentioned above,
- second, a non forecast improvement which should emerge as the number of certified federates is increasing and additional experience is gained with new nations being involved in the certification process bringing different perspectives and mentalities. Paragraph 4.6 provides examples of such improvements.

Currently the US is the unique nation dealing with the HLA certification process. When non-US nations join the process, it is considered that future evolutions should be decided on a consensus basis to ensure that a common testing suite is maintained by participating nations. The task group proposes that a user/tester club (or working group) should be established. This group should meet once or twice a year and would be tasked to propose, discuss and decide the necessary evolution of the HLA certification process and of the supporting software, according to the existing technical and political constraints.

It is considered that the US should chair this future working group since this nation is internationally recognised as the leader for this activity. Participating task group nations recommend that this supporting organisation should be integrated within the NMSG, although the task group recognises that it is also possible to establish it in another military (NATO/national) or non-military organisation such as IEEE or SISO.

### 6.4. Next Step Proposals

The schedule for TG-008 to report on the present study is end 2001. It is proposed that a new task group be set up to establish and initiate the corresponding “users/testers club” as described in paragraph 6.3. It is recommended in compliance with the RTO procedures, that an “exploratory team” be formed by mid-2002. This will avoid the dispersion of the important expertise which has been gathered in TG-008. This exploratory team should draft the terms of reference for the future “users/testers club”. The MSCO is volunteering to chair this exploratory team.

A primary and very important step for the establishment of the future NATO HLA certification activity is the agreement by individual nations to establish national capabilities. Establishing such a capability requires not only an investment in hardware and software as described in paragraph 2.2, but also primarily human resources: the importance of dedicated human resources is strongly emphasised. In addition, it is also important that future testers be educated and trained: this requires an urgent coordination between nations in addition to the rapid decision of non-US nations to establish a national certification activity.

## **Annex A**

### **US Technical Area Task (TAT) Process**

- The point of contact (POC) assists the client (Requesting Activity) in scoping the work and preparing a Statement of Work (SOW).
- POC (either government or employee) notifies the Technical Area Task (TAT) Manager of a potential TAT, and provides him with RA contact information.
- TAT Manager/Asst. TAT Manager meets with Contracting Officer's Technical Representative (COTR) to gain concurrence that the TAT is within the technical scope of the contract using the draft SOW as the means of communication. This concurrence is needed before the process can proceed.
- Once the COTR (DMSO) concurs, the TAT Manager/Asst. TAT Manager assists client and the POC in developing the final SOW.
- TAT Manager/Asst. TAT Manager provides POC and requesting activity with all the contact information, and funding instructions (and example).
- The TAT Manager/Asst. TAT Manager will enter the TAT and a Statement of Work (SOW) into the Information Analysis Center (IAC) electronic tracking system.
- The COTR forwards the SOW to the IAC Program Manager (PM) (re: Defense Technical Information Center, DTIC). The IAC PM either approves or disapproves the IAC Work Plan. If approved, IITRI will be prompted to submit a technical and cost proposal.
- The requesting activity is provided the costing information. They prepare and forward a Military Interdepartmental Purchase Request (MIPR) to the Defense Supply Center Columbus (DSCC).
- The TAT Manager/Asst. TAT Manager prepares technical proposals for the SOW and submits to the POC for final approval.
- TAT Manager/Asst. TAT Manager, with contract's assistance, completes the technical and cost proposal.
- TAT Manager/Asst. TAT Manager enters cost and technical proposals into electronic tracking system.
- IITRI Contracts submits the final Technical and Cost Proposals to DSCC, the requesting activity, and the COTR for approval.
- The requesting activity and COTR review proposal. The Requesting Activity provides the COTR a verbal/email/faxed approval of the proposal. The COTR will then approve the proposals and forward (electronically) to DSCC.
- The Government Contracting Officer will then prepare the contract Task Order for approval, and mails to IITRI contracting for signature.
- IITRI Contracting signs contract modification.
- Procurement Contracting Officer approves and issues new task order.
- Task Order goes to IITRI Contract Administrator, who notifies TAT Manager/Asst. TAT Manager and Project Controller. TAT Manager/Asst. TAT Manager co-ordinates with Project Controller and Program Manager to set up charge numbers and initiate work.

**This page has been deliberately left blank**

---

**Page intentionnellement blanche**

## Annex B

### US Subscription Account Process

The subscription account allows the customer to deposit a prescribed set of funding for the performance of a task. As individuals execute the task time, travel or other expensive the account is drawn down accordingly. For example, if NATO establishes a subscription account with \$50K the MSIAC would conduct HLA compliance testing on Federates that NATO approves until all funding is exhausted. Below is the format for establishing a subscription account work plan.

#### DEPARTMENT OF DEFENSE (DoD) INFORMATION ANALYSIS CENTER (IAC) SUBSCRIPTION WORK PLAN

Work Plan Number: \_\_\_\_\_

Date:

Task Title: Provide Technical Support for?

IAC POC: Jamie Gardner

Phone: 703-933-3315

Fax: 703-933-3325

Email: [jgardner@msiac.dmsso.mil](mailto:jgardner@msiac.dmsso.mil), [jgardner@iitri.org](mailto:jgardner@iitri.org)

Fiscal: Daniel Rodgers

Phone: 614-692-7119

Fax: 614-692-6935

Email: [daniel\\_rodgers@dsccl.dla.mil](mailto:daniel_rodgers@dsccl.dla.mil)

Requesting Activity and Address:

?

Attn:

Address:

Address

Technical POC:

Phone:

Fax:

Email:

Financial POC: Gary Yerace

Phone: (703) 998-0660

Fax: (703) 998-0664

Email: [gyerace@dmsso.mil](mailto:gyerace@dmsso.mil)

## SPECIFIC TASK: Brief Description

Estimated cost: \$xxx

Estimated man-hours: x

Estimated duration: x

Approval Signature (RA) \_\_\_\_\_ Date \_\_\_\_\_

Technical Monitor (COTR) \_\_\_\_\_ Date \_\_\_\_\_

Items that need to be agreed upon are the Task Title, Task Description, and Estimated Duration. The cost will be determined by the IAC POC based upon the task description, labour, travel (if required) and duration of the task. Work could begin on a subscription account in as little as two weeks.

## Annex C

### List of Acronyms

<b>AAR</b>	After Action Review
<b>API</b>	Application Programming Interface
<b>ARCOSIM</b>	<i>ARchitecture COMmune de SIMulation</i> (France)
<b>BWB</b>	<i>Bundesamt für Wehrtechnik und Beschaffung</i> (the German Federal Office for Defence Technology and Procurement)
<b>CA</b>	Certification Agent (HLA Certification)
<b>CATT</b>	Combined Arms Tactical Trainer
<b>CAX</b>	Computer Assisted Exercise
<b>CD</b>	Compact Disk
<b>CD-ROM</b>	Compact Disk- Read Only memory
<b>CNAD</b>	Conference of National Armament Directors
<b>CORBA</b>	Common Object Request Broker Architecture
<b>COTR</b>	Contracting Officer's Technical Representative
<b>COTS</b>	Commercial Off The Shelf
<b>CS</b>	Conformance Statement (HLA Certification)
<b>CSI</b>	Combat Systems Integration (UK)
<b>CSR</b>	Certification Summary Report
<b>CTF</b>	Common Technical Framework
<b>C4I</b>	Command, Control, Communications, Computers & Information
<b>DDM</b>	Data Distribution Management
<b>DGA</b>	<i>Délégation Générale pour l'Armement</i> (French procurement agency)
<b>DMSO</b>	Defense Modeling & Simulation Office (US DoD)
<b>DIS</b>	Distributed Interactive Simulation (IEEE standard 1278)
<b>DiMuNDS</b>	
<b>DoD</b>	U.S. Department of Defense
<b>DSCC</b>	Defense Supply Center Columbus
<b>DSS</b>	Decision Support Systems
<b>DSTI</b>	Defence Science & Technology laboratory (UK)
<b>DTIC</b>	Defense Technical Information Center
<b>ESCADRE</b>	<i>Environnement de Simulation en Conception Orientée Objet &amp; Ada95 pour le Développement et la Réutilisation des Etudes</i> (France)
<b>FCTT</b>	Federate Compliance Testing Tool (HLA Certification)
<b>FED</b>	Federation Execution Data
<b>FEDEP</b>	Federation Development and Execution Process (HLA)
<b>FOAS</b>	Future Offensive Air System
<b>FOM</b>	Federation Object Model (HLA)
<b>FTMS</b>	Federate Test Management System (HLA Certification)
<b>FR</b>	France
<b>FUT</b>	Federate Under Test (HLA Certification)
<b>FTP</b>	Federate Testing Process

<b>FYROM</b>	Former Yugoslavian Republic Of Macedonia
<b>FVT</b>	Federate Verification Tool (HLA)
<b>GE</b>	Germany
<b>GERTICO</b>	German RTI based on CORBA
<b>GFE</b>	Government Furniture and Equipment
<b>GOTS</b>	Government Off The Shelf
<b>GRIM</b>	Guidance, Rationale and Interoperability Modalities (RPR-FOM)
<b>HLA</b>	High Level Architecture (US DoD standard 1.3, IEEE standard 1516)
<b>IAC</b>	Information Analysis Center
<b>IDL</b>	Interface Definition Language (CORBA)
<b>IEEE</b>	Institute of Electrical and Electronic Engineers
<b>IF</b>	Interface
<b>IGBAD</b>	Integrated Ground Based Air Defence (UK)
<b>IITRI</b>	Illinois Institute of Technology Research Institute
<b>IP</b>	Internet Protocol
<b>I&amp;S</b>	Infrastructure and Services
<b>ISES</b>	International Synthetic Environment Symposium (UK)
<b>ISP</b>	Internet Service Provider
<b>IT</b>	Information Technology
<b>ITEC</b>	International Training and Education Conference
<b>JTLS</b>	Joint Theatre Level Simulation
<b>JUDS</b>	Joint UK/US Distributed Simulation
<b>LAN</b>	Local Area Network
<b>MC</b>	NATO Military Committee
<b>MIPR</b>	Military Interdepartmental Purchase Request
<b>MoA</b>	Memorandum of Agreement
<b>MoD</b>	Ministry of Defence
<b>MoU</b>	Memorandum of Understanding
<b>MS</b>	Microsoft
<b>M&amp;S</b>	Modelling & Simulation
<b>MSAP</b>	Modelling & Simulation Action Plan
<b>MSCO</b>	Modelling & Simulation Co-ordination Office (NATO)
<b>MSG</b>	Modelling & Simulation Group
<b>MSHATF</b>	Medium Support Helicopter Aircrew Training Facility
<b>MSIAC</b>	Modeling and Simulation Information Analysis Center (U.S.)
<b>MSMP</b>	Modelling and Simulation Master Plan
<b>NAAG</b>	NATO Army Armaments Group
<b>NAC</b>	North-Atlantic Council
<b>NACC</b>	North Atlantic Co-operation Council
<b>NATO</b>	North Atlantic Treaty Organization
<b>NC3A</b>	NATO Consultation, Command and Control Agency
<b>NFSE</b>	National Focus for Synthetic Environments (UK)
<b>NMSG</b>	NATO Modelling and Simulation Group
<b>NT</b>	New Technology

<b>OSCE</b>	Organisation for Security and Co-operation in Europe
<b>OML</b>	Object Model Library
<b>OMRC</b>	Object Model Resource Center
<b>OMT</b>	Object Model Template (HLA)
<b>PC</b>	Personal Computer
<b>PfP</b>	Partnership (or Partners) for Peace
<b>POC</b>	Point Of Contact
<b>POW</b>	Program Of Work
<b>ΨSA</b>	Proposed Standard Interface for Simulation Applications (Germany)
<b>RAL</b>	RTI Abstraction Layer
<b>RAM</b>	Random Access Memory
<b>RepSOM</b>	Representative SOM
<b>R&amp;D</b>	Research and Development
<b>RFP</b>	Request For Proposal
<b>RID</b>	RTI Initialisation Data
<b>RPR-FOM</b>	Real-Time Platform Reference Federation Object Model
<b>RTA</b>	Research and Technology Agency (NATO)
<b>RTI</b>	Run-Time Infrastructure (HLA)
<b>RTO</b>	Research and Technology Organisation (NATO)
<b>SBA</b>	Simulation Based Acquisition
<b>SDE</b>	Shared Data Environment
<b>SDR</b>	Strategic Defence Review (UK)
<b>SE</b>	Synthetic Environment
<b>SEBA</b>	SE Based Acquisition (UK)
<b>SECO</b>	UK Synthetic Environments Coordination Office
<b>SEMS</b>	Synthetic Environments, Modelling and Simulation
<b>SGMS</b>	Steering Group for M&S
<b>SINCE</b>	Simulation and C2 Information Systems Interconnectivity Experiment
<b>SISO</b>	Simulation Interoperability Standards Organization
<b>SIW</b>	Simulation Interoperability Workshop (SISO)
<b>SME</b>	Subject Matter Expert
<b>SPI</b>	Smart Procurement Initiative (UK)
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SOW</b>	Statement Of Work
<b>SOM</b>	Simulation Object Model( HLA)
<b>STANAG</b>	Standardisation Agreement (NATO)
<b>TAP</b>	Technical Activity Proposal
<b>TAT</b>	Technical Area Task
<b>T&amp;E</b>	Testing and Evaluation
<b>TG</b>	Task Group
<b>TOR</b>	Terms Of Reference
<b>UML</b>	Unified Modeling Language
<b>UN</b>	United Nations
<b>UK</b>	United Kingdom



<b>US</b>	United States of America
<b>VNC</b>	Voluntary National Contribution
<b>VR</b>	Virtual Reality
<b>WAN</b>	Wide Area Network
<b>WTD 81</b>	BWB Technical Center for Communication and Electronics (Germany)

## **Annex D**

### **References**

- [1] Paul Kaminski, "DoD High Level Architecture (HLA) for Simulations," USD(A&T) Memorandum, 10 September 1996
- [2] Jacques Gansler, "DoD Transition to the High Level Architecture (HLA) for Simulations," USD(A&T) Memorandum, 1 April 1998
- [3] US Department of Defense, "High Level Architecture Rules Version 1.3," 20 April 1998
- [4] US Department of Defense, "High Level Architecture Interface Specification Version 1.3," 20 April 1998
- [5] US Department of Defense, "High Level Architecture Object Model Template Specification Version 1.3," 20 April 1998
- [6] IEEE 1516-2000 : "IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Framework and Rules"
- [7] IEEE 1516.1-2000 : "IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Federate Interface Specification"
- [8] IEEE1516.2-2000 : "IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) - Object Model Template (OMT) Specification"
- [9] Simulation Interoperability Workshop, paper #00F-SIW-036, "Improvements to the HLA Federate Compliance Testing Process", by Margaret M. Horst, David Rosenbaum, Kyle A. Crawford, Georgia Tech Research Institute, September 2000

**This page has been deliberately left blank**



**Page intentionnellement blanche**

REPORT DOCUMENTATION PAGE			
<b>1. Recipient's Reference</b>	<b>2. Originator's References</b> RTO-TR-050 AC/323(NMSG-011)TP/03	<b>3. Further Reference</b> ISBN 92-837-1087-8	<b>4. Security Classification of Document</b> UNCLASSIFIED/ UNLIMITED
<b>5. Originator</b>	Research and Technology Organisation North Atlantic Treaty Organisation BP 25, F-92201 Neuilly-sur-Seine Cedex, France		
<b>6. Title</b>	NATO HLA Certification		
<b>7. Presented at/sponsored by</b>	the RTO NATO Modelling and Simulation Group Task Group 008.		
<b>8. Author(s)/Editor(s)</b> Multiple	<b>9. Date</b> June 2002		
<b>10. Author's/Editor's Address</b> Multiple	<b>11. Pages</b> 54		
<b>12. Distribution Statement</b>	There are no restrictions on the distribution of this document. Information about the availability of this and other RTO unclassified publications is given on the back cover.		
<b>13. Keywords/Descriptors</b> High Level Architecture (HLA) HLA Certification Interoperability Standards Modelling and Simulation (M&S)			
<b>14. Abstract</b>  <p>The Report from the NATO Modelling and Simulation Steering Group approved by the North-Atlantic Council establishes the need for a common (open standard) technical framework (CTF) to promote the interoperability and reuse of models and simulations across the Alliance. MSMP Sub-objective 1.1, "Adopt the High Level Architecture (HLA) as the NATO standard technical architecture for simulation applications," provides the best available technical architecture to satisfy this need.</p> <p>HLA is recognised as a critical and necessary enabler for the interoperability and reuse of simulations. There is a need to acquire some guarantee that so-called "HLA-based" simulations are, in fact, HLA-compliant in accordance with applicable standards in order to attain those stages of interoperability and reuse. This report compares three different solutions to implement a NATO certification capability. The recommended solution is to establish national capabilities within voluntary nations. In order to co-ordinate and supervise this distributed implementation, it is required to establish a users/testers group to be created within the NMSG organisation.</p>			

**This page has been deliberately left blank**



**Page intentionnellement blanche**



## RESEARCH AND TECHNOLOGY ORGANISATION

BP 25 • 7 RUE ANCELLE

F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE

Télécopie 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

## DIFFUSION DES PUBLICATIONS

RTO NON CLASSIFIÉES

L'Organisation pour la recherche et la technologie de l'OTAN (RTO), détient un stock limité de certaines de ses publications récentes, ainsi que de celles de l'ancien AGARD (Groupe consultatif pour la recherche et les réalisations aérospatiales de l'OTAN). Celles-ci pourront éventuellement être obtenues sous forme de copie papier. Pour de plus amples renseignements concernant l'achat de ces ouvrages, adressez-vous par lettre ou par télécopie à l'adresse indiquée ci-dessus. Veuillez ne pas téléphoner.

Des exemplaires supplémentaires peuvent parfois être obtenus auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la RTO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus sur la liste d'envoi de l'un de ces centres.

Les publications de la RTO et de l'AGARD sont en vente auprès des agences de vente indiquées ci-dessous, sous forme de photocopie ou de microfiche. Certains originaux peuvent également être obtenus auprès de CASI.

## CENTRES DE DIFFUSION NATIONAUX

## ALLEMAGNE

Streitkräfteamt / Abteilung III  
Fachinformationszentrum der  
Bundeswehr, (FIZBw)  
Friedrich-Ebert-Allee 34  
D-53113 Bonn

## BELGIQUE

Etat-Major de la Défense  
Département d'Etat-Major Stratégie  
ACOS-STRAT-STE – Coord. RTO  
Quartier Reine Elisabeth  
Rue d'Evère, B-1140 Bruxelles

## CANADA

Services d'information scientifique  
pour la défense (SISD)  
R et D pour la défense Canada  
Ministère de la Défense nationale  
Ottawa, Ontario K1A 0K2

## DANEMARK

Danish Defence Research Establishment  
Ryvangs Allé 1, P.O. Box 2715  
DK-2100 Copenhagen Ø

## ESPAGNE

INTA (RTO/AGARD Publications)  
Carretera de Torrejón a Ajalvir, Pk.4  
28850 Torrejón de Ardoz - Madrid

## ETATS-UNIS

NASA Center for AeroSpace  
Information (CASI)  
Parkway Center  
7121 Standard Drive  
Hanover, MD 21076-1320

## FRANCE

O.N.E.R.A. (ISP)  
29, Avenue de la Division Leclerc  
BP 72, 92322 Châtillon Cedex

## GRECE (Correspondant)

Hellenic Ministry of National  
Defence  
Defence Industry Research &  
Technology General Directorate  
Technological R&D Directorate  
D.Soutsou 40, GR-11521, Athens

## HONGRIE

Department for Scientific  
Analysis  
Institute of Military Technology  
Ministry of Defence  
H-1525 Budapest P O Box 26

## ISLANDE

Director of Aviation  
c/o Flugrad  
Reykjavik

## ITALIE

Centro di Documentazione  
Tecnico-Scientifica della Difesa  
Via XX Settembre 123a  
00187 Roma

## LUXEMBOURG

Voir Belgique

## NORVEGE

Norwegian Defence Research  
Establishment  
Attn: Biblioteket  
P.O. Box 25, NO-2007 Kjeller

## PAYS-BAS

NDRCC  
DGM/DWOO  
P.O. Box 20701  
2500 ES Den Haag

## POLOGNE

Chief of International Cooperation  
Division  
Research & Development Department  
218 Niepodleglosci Av.  
00-911 Warsaw

## PORTUGAL

Estado Maior da Força Aérea  
SDFA - Centro de Documentação  
Alfragide  
P-2720 Amadora

## REPUBLIQUE TCHEQUE

DIC Czech Republic-NATO RTO  
VTÚL a PVO Praha  
Mladoboleslavská ul.  
Praha 9, 197 06, Česká republika

## ROYAUME-UNI

Dstl Knowledge Services  
Kentigern House, Room 2246  
65 Brown Street  
Glasgow G2 8EX

## TURQUIE

Millî Savunma Başkanlığı (MSB)  
ARGE Dairesi Başkanlığı (MSB)  
06650 Bakanlıklar - Ankara

## AGENCES DE VENTE

## NASA Center for AeroSpace

Information (CASI)  
Parkway Center  
7121 Standard Drive  
Hanover, MD 21076-1320  
Etats-Unis

## The British Library Document

Supply Centre  
Boston Spa, Wetherby  
West Yorkshire LS23 7BQ  
Royaume-Uni

## Canada Institute for Scientific and

Technical Information (CISTI)  
National Research Council  
Acquisitions  
Montreal Road, Building M-55  
Ottawa K1A 0S2, Canada

Les demandes de documents RTO ou AGARD doivent comporter la dénomination "RTO" ou "AGARD" selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications RTO et AGARD figurent dans les journaux suivants:

## Scientific and Technical Aerospace Reports (STAR)

STAR peut être consulté en ligne au localisateur de  
ressources uniformes (URL) suivant:  
<http://www.sti.nasa.gov/Pubs/star/Star.html>  
STAR est édité par CASI dans le cadre du programme  
NASA d'information scientifique et technique (STI)  
STI Program Office, MS 157A  
NASA Langley Research Center  
Hampton, Virginia 23681-0001  
Etats-Unis

## Government Reports Announcements &amp; Index (GRA&amp;I)

publié par le National Technical Information Service  
Springfield  
Virginia 2216  
Etats-Unis  
(accessible également en mode interactif dans la base de  
données bibliographiques en ligne du NTIS, et sur CD-ROM)





## RESEARCH AND TECHNOLOGY ORGANISATION

BP 25 • 7 RUE ANCELLE

F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE

Telefax 0(1)55.61.22.99 • E-mail mailbox@rta.nato.int

## DISTRIBUTION OF UNCLASSIFIED

## RTO PUBLICATIONS

NATO's Research and Technology Organisation (RTO) holds limited quantities of some of its recent publications and those of the former AGARD (Advisory Group for Aerospace Research & Development of NATO), and these may be available for purchase in hard copy form. For more information, write or send a telefax to the address given above. **Please do not telephone.**

Further copies are sometimes available from the National Distribution Centres listed below. If you wish to receive all RTO publications, or just those relating to one or more specific RTO Panels, they may be willing to include you (or your organisation) in their distribution.

RTO and AGARD publications may be purchased from the Sales Agencies listed below, in photocopy or microfiche form. Original copies of some publications may be available from CASI.

## NATIONAL DISTRIBUTION CENTRES

## BELGIUM

Etat-Major de la Défense  
Département d'Etat-Major Stratégie  
ACOS-STRAT-STE – Coord. RTO  
Quartier Reine Elisabeth  
Rue d'Evère, B-1140 Bruxelles

## CANADA

Defence Scientific Information  
Services (DSIS)  
Defence R&D Canada  
Department of National Defence  
Ottawa, Ontario K1A 0K2

## CZECH REPUBLIC

DIC Czech Republic-NATO RTO  
VTÚL a PVO Praha  
Mladoboleslavská ul.  
Praha 9, 197 06, Česká republika

## DENMARK

Danish Defence Research  
Establishment  
Ryvangs Allé 1, P.O. Box 2715  
DK-2100 Copenhagen Ø

## FRANCE

O.N.E.R.A. (ISP)  
29 Avenue de la Division Leclerc  
BP 72, 92322 Châtillon Cedex

## GERMANY

Streitkräfteamt / Abteilung III  
Fachinformationszentrum der  
Bundeswehr, (FIZBw)  
Friedrich-Ebert-Allee 34  
D-53113 Bonn

## GREECE (Point of Contact)

Hellenic Ministry of National  
Defence  
Defence Industry Research &  
Technology General Directorate  
Technological R&D Directorate  
D.Soutsou 40, GR-11521, Athens

## HUNGARY

Department for Scientific  
Analysis  
Institute of Military Technology  
Ministry of Defence  
H-1525 Budapest P O Box 26

## ICELAND

Director of Aviation  
c/o Flugrad  
Reykjavik

## ITALY

Centro di Documentazione  
Tecnico-Scientifica della Difesa  
Via XX Settembre 123a  
00187 Roma

## LUXEMBOURG

See Belgium

## NETHERLANDS

NDRCC  
DGM/DWOO  
P.O. Box 20701  
2500 ES Den Haag

## NORWAY

Norwegian Defence Research  
Establishment  
Attn: Biblioteket  
P.O. Box 25, NO-2007 Kjeller

## POLAND

Chief of International Cooperation  
Division  
Research & Development  
Department  
218 Niepodleglosci Av.  
00-911 Warsaw

## PORTUGAL

Estado Maior da Força Aérea  
SDFA - Centro de Documentação  
Alfragide  
P-2720 Amadora

## SPAIN

INTA (RTO/AGARD Publications)  
Carretera de Torrejón a Ajalvir, Pk.4  
28850 Torrejón de Ardoz - Madrid

## TURKEY

Millî Savunma Başkanlığı (MSB)  
ARGE Dairesi Başkanlığı (MSB)  
06650 Bakanlıklar - Ankara

## UNITED KINGDOM

Dstl Knowledge Services  
Kentigern House, Room 2246  
65 Brown Street  
Glasgow G2 8EX

## UNITED STATES

NASA Center for AeroSpace  
Information (CASI)  
Parkway Center  
7121 Standard Drive  
Hanover, MD 21076-1320

## SALES AGENCIES

NASA Center for AeroSpace  
Information (CASI)

Parkway Center  
7121 Standard Drive  
Hanover, MD 21076-1320  
United States

The British Library Document  
Supply Centre

Boston Spa, Wetherby  
West Yorkshire LS23 7BQ  
United Kingdom

Canada Institute for Scientific and  
Technical Information (CISTI)

National Research Council  
Acquisitions  
Montreal Road, Building M-55  
Ottawa K1A 0S2, Canada

Requests for RTO or AGARD documents should include the word 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of RTO and AGARD publications are given in the following journals:

## Scientific and Technical Aerospace Reports (STAR)

STAR is available on-line at the following uniform  
resource locator:

<http://www.sti.nasa.gov/Pubs/star/Star.html>

STAR is published by CASI for the NASA Scientific  
and Technical Information (STI) Program  
STI Program Office, MS 157A  
NASA Langley Research Center  
Hampton, Virginia 23681-0001  
United States

## Government Reports Announcements &amp; Index (GRA&amp;I)

published by the National Technical Information Service  
Springfield  
Virginia 22161  
United States  
(also available online in the NTIS Bibliographic  
Database or on CD-ROM)



Printed by St. Joseph Print Group Inc.  
(A St. Joseph Corporation Company)

1165 Kenaston Street, Ottawa, Ontario, Canada K1G 6S1